

**Étude et mise en place d’un réseau d’entreprise**

SHEN Liangyi

SURESH Aravind

WANG Jing

WANG Meibao

WANG Miaojie

XIAO Wenbo

Summary

[**1.Introduction**](#_gbcz1xrvr35g) **3**

[**2. Demande analyse**](#_t227owetltyy) **4**

[2.1 Background of the project](#_hmj3facismas) 4

[2.2 Client demands](#_vzp4gb1xgs5z) 4

[2.3 Construction](#_9ld83s9l57te) 4

[2.3.1 Company structure](#_1d00uxqrqeiz) 4

[2.3.2 Vlan division](#_5ftod8ahui1k) 5

[2.3.2 Company network structure](#_kgwnvcq4durc) 6

[2.4 Equipments and Budgets](#_fjiehe27uws5) 9

[**3. Internal Solution**](#_c4flgsa2i5fq) **11**

[3.1 Access Layer : VLAN](#_1fz9q0cz080t) 11

[3.1.1 Principle](#_1j8jlemcbypp) 11

[3.1.2. Advantages of VLAN](#_31326zh9y3a5) 12

[3.2. Distributed layer : VSS](#_l3ssfp5o75kx) 13

[3.2.1. Principle](#_vzall4nl11nw) 13

[3.2.2 Advantages](#_bm0w93t12le6) 13

[3.3 MSTP+VRRP](#_rk54vwa63f5o) 14

[3.3.1. MSTP](#_22dxin9ehr5f) 14

[3.3.2. MSTP Advantages](#_ii72boah3t58) 14

[3.3.3. VRRP](#_dhm52gj8fmyx) 14

[3.3.4. VRRP Advantages](#_xu8d4l869bdg) 15

[3.3.5. VRRP work with MSTP](#_vg7hugq3py54) 15

[3.4 Core Layer: OSPF](#_6sowvgj585s4) 16

[3.4.1 OSPF Routing Protocols](#_faipthtl2hdw) 16

[3.4.2 FIREWALL](#_dcfha5muf44r) 18

[3.4.3 NAT](#_ct5iddhv2wd6) 19

[3.4.4 Static NAT](#_qzv8drrh3y40) 19

[3.4.5 Dynamic NAT](#_qzv8drrh3y40) 20

[3.4.5 ACL](#_qzv8drrh3y40) 20

[3.4.6 DMZ](#_ifg4x9toxes4) 21

[3.5 SERVER](#_qzv8drrh3y40) 23

[3.5.1 LDAP](#_td6ypqp7hhvw) 23

[3.5.2 DHCP](#_f13fynnmjkgy) 24

[3.5.3 DNS](#_qzv8drrh3y40) 26

[3.6 External network](#_8z0h3zdj91fw) 28

[3.6.1 BGP+IS-IS](#_1fz9q0cz080t) 28

[3.6.2 MPLS VPN](#_bpvxabphj7iw) 28

[**4. Special functions**](#_sbkn7f2masyy) **30**

[4.1 IPv6 to IPv4](#_iu59spcznf7y) 30

[4.1.1 Generale Advantages of tunneling](#_y3sj7pad9dj4) 30

[4.2 VoIP](#_h7qny32mqu79) 31

[**5.Simulation on GNS3 and VMware**](#_izwzg8r6wrg) **33**

[5.1 Architecture](#_tmu6cbifpt9r) 33

[5.2 Results](#_pabz1b82k4wl) 39

[**References**](#_wy79yflz4gyl) **44**

# 

# 

# 1.Introduction

A network constructure is an important part of a company. Including the selections of various protocols and equipment. In this project, a design of network is proposed according to requests.

# 2. Demande analyse

## 2.1 Background of the project

An internationally oriented French company launches RFP (Request For Proposal) to design their computer network. This company has 2 remote sites on 2 different campuses: one in Lyon and one in Tokyo, with several offices (Management, Accounting, Services, IT..).

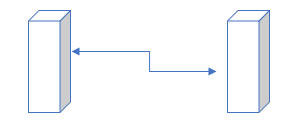
## 2.2 Client demands

* The network requires high reliability, stability and redundancy.
* Two campuses can communicate to each other.
* Different VLANs can communicate with each other.
* The internal computers of the company only can contact by internal mail.
* Use VPN to keep communication with overseas campus.
* Definition of an IPv6 and IPv4 hybrid addressing scheme with an implementation of 6to4.
* Implementation of the Virtual Switching System (VSS) technology, allowing to deploy a level 2 topology by avoiding spanning tree problems
* Establishment of services (mail server, DHCP, DNS ...)

## 2.3 Construction

### 2.3.1 Company structure

There are two campuses of the company, one site is in Lyon and another one is in Tokyo. Each of the campus has five departments which are Management, Accounting, Services, IT and Marketing in the same building.



Size of the company :

|  |  |  |  |
| --- | --- | --- | --- |
| Campus | Floors | Department | the number of people for each department |
| Head Office | 7 | 7 | 40 |
| Branch company | 5 | 5 | 40 |

### 

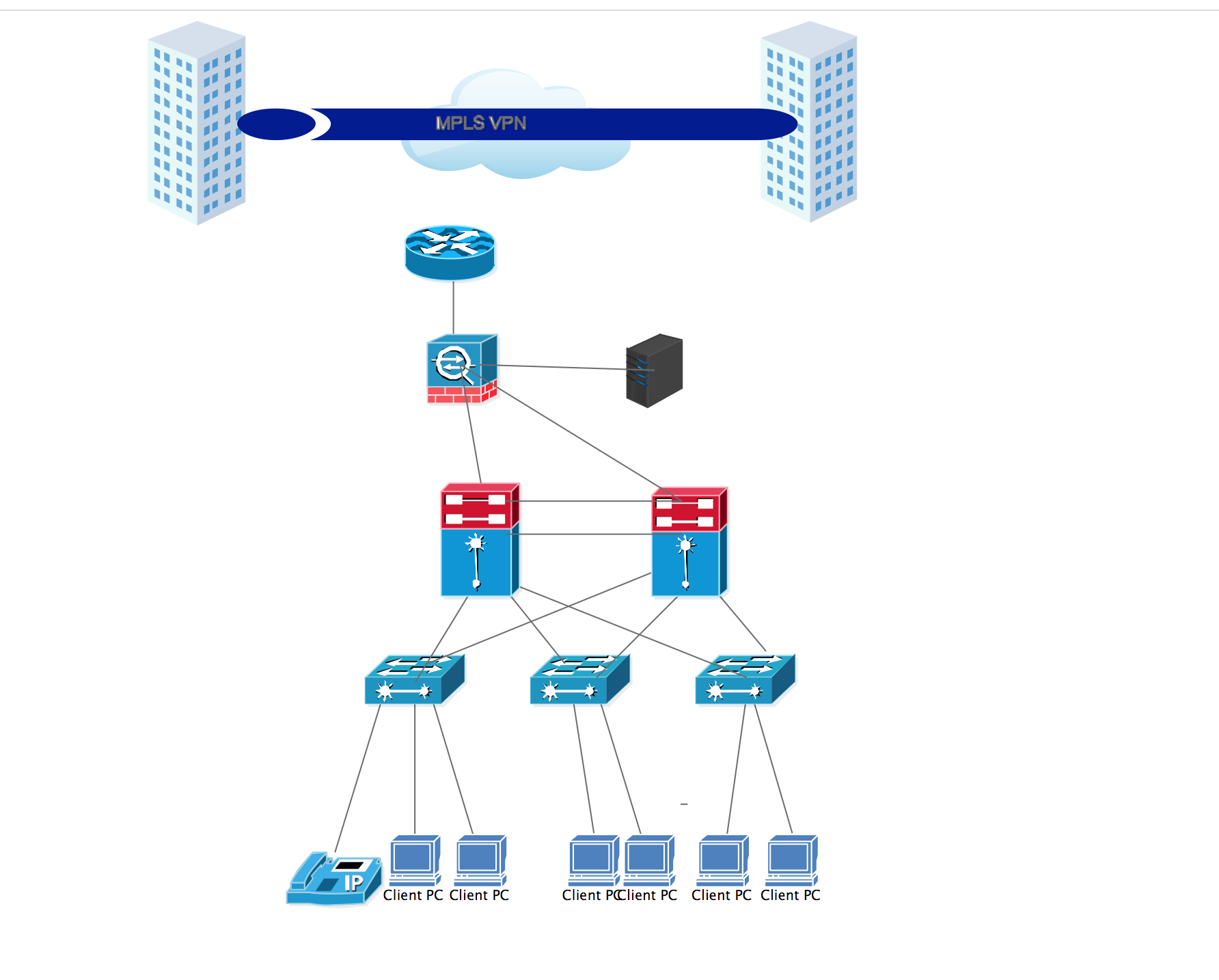
### 2.3.2 Vlan division

In this structure, every department belong to one vlan. On the one hand, vlan is used to decrease the size of the broadcast, which can reduce network overhead and response time. On the other hand, it can protect the security of each department.

|  |  |  |
| --- | --- | --- |
| Network | Fonction | Vlan |
| 172.16.10.1/24 - 172.16.10.100/24 | Department 1 | 10 |
| 172.16.10.101/24 -  172.16.10.200/24 | Department 2 | 20 |
| 172.16.20.1/24 -  172.16.20.100/24 | Department 3 | 30 |
| 172.16.20.101/24 -  172.16.20.200/24 | Department 4 | 40 |
| 172.16.30.1/24 -  172.16.30.100/24 | Department 5 | 50 |
| 172.16.30.101/24 -  172.16.30.200/24 | Department 6 | 60 |
| 172.16.40.1/24-  172.16.40.101/24 | Department 7 | 70 |
| 172.16.50.1/24 -  172.16.50.100/24 | VoIP | 80 |
| 172.16.50.101/24 -  172.16.50.200/24 | VoIP | 90 |
| 172.16.60.1/24 -  172.16.60.100/24 | Printer | 100 |
| 172.16.70.1/24 -  172.16.70.254/24 | Backup | 110 |

### 2.3.2 Company network structure

This design divides the internal network into three parts: Core Layer, Distribution layer, Access Layer. And can provide a clear division of each layer to adapt to the complex environment.



**Core Layer** : This layer is considered the backbone of the network and includes the high-end switches and high-speed cables such as fiber cables. This layer of the network does not route traffic at the LAN. In addition, no packet manipulation is done by devices in this layer. Rather, this layer is concerned with speed and ensures reliable delivery of packets. The factors to be considered while designing devices to be used in the core layer are:

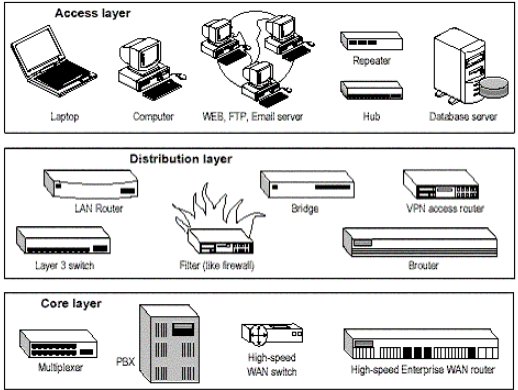
* High data transfer rate: Speed is important at the core layer. One way that core networks enable high data transfer rates is through load sharing, where traffic can travel through multiple network connections.
* Low latency period: The core layer typically uses high-speed low latency circuits which only forward packets and do not enforcing policy.
* High reliability: Multiple data paths ensure high network fault tolerance; if one path experiences a problem, then the device can quickly discover a new route.
* Cable : Optical fibers and serial cable.

**Distribution layer**: This layer includes LAN-based routers and layer 3 switches. This layer ensures that packets are properly routed between subnets and VLANs in enterprise. This layer is also called the Workgroup layer. Mainly responsible for routing. It also provides policy-based network connectivity, including:

* Packet filtering (firewalling): Processes packets and regulates the transmission of packets based on its source and destination information to create network borders.
* QoS: The router or layer 3 switches can read packets and prioritize delivery, based on policies you set.
* Access Layer Aggregation Point: The layer serves the aggregation point for the desktop layer switches.
* Control Broadcast and Multicast: The layer serves as the boundary for broadcast and multicast domains.
* Application Gateways: The layer allows you to create protocol gateways to and from different network architectures.
* The distribution layer also performs queuing and provides packet manipulation of the network traffic.
* Cable: Optical fiber and CAT-6.

**Access layer**: This layer includes hubs and switches. This layer is also called the desktop layer because it focuses on connecting client nodes, such as workstations to the network. This layer ensures that packets are delivered to end user computers. At the access layer, you can:

* Enable MAC address filtering: It is possible to program a switch to allow only certain systems to access the connected LANs.
* Create separate collision domains: A switch can create separate collision domains for each connected node to improve performance.
* Share bandwidth: You can allow the same network connection to handle all data.
* Handle switch bandwidth: You can move data from one network to another to perform load balancing.



each layer might comprise more than two devices or a single device might function across multiple layers. The benefits of the Cisco hierarchical model include:

* High Performance: You can design high performance networks, where only certain layers are susceptible to congestion.
* Efficient management & troubleshooting: Allows you to efficiently organize network management and isolate causes of network trouble.
* Policy creation: You can easily create policies and specify filters and rules.
* Scalability: You can grow the network easily by dividing your network into functional areas.
* Behavior prediction: When planning or managing a network, the model allows you determine what will happen to the network when new stresses are placed on it.
* Cable: CAT-6

## 2.4 Equipments and Budgets

* Core Layer router:Cisco WS-C3560X-48P-S
* Access Layer router:Cisco WS-C2960X-48TS-LL
* Firewall:CISCO ASA5520-BUN-K9
* IP phone:CISCO CP-6921
* Server:IBM System x3650 M5(5462I05)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Types | Models | Price | numbers | Total price(€) |
| Core Layer | Cisco WS-C3560X-48P-S | 2700 | 4 | 10800 |
| Access Layer | Cisco  WS-C2960S-48TS-S | 800 | 12 | 9600 |
| Firewall | CISCO ASA5520-BUN-K9 | 2200 | 2 | 4400 |
| IP Phone | CISCO CP-6921 | 100 | 36 | 3600 |
| Server | IBM System x3650 M5(5462I05) | 3000 | 1 | 3000 |
| Wiring System | Voice patch panel,RJ45 patch panel,Fiber patch panels,  Wall-type dual-port panel,Cable patch panels and cabinets,  Optical fiber production supplies,Cat-6,Jumper wire,Single-mode fiber,Metal pipe, etc... |  |  | 80000 |
| Total |  |  |  | 112400 |

# 

# 3. Internal Solution

## 3.1 Access Layer : VLAN

### 3.1.1 Principle

VLAN (Virtual LAN) is a Local Area Network, provides the nodes connected to it with direct([Layer 2](http://searchnetworking.techtarget.com/definition/layer-2)) access to one another. It is usually comprised of one or more [Ethernet](http://searchnetworking.techtarget.com/definition/Ethernet) switches. Computers on different LANs talk to each other using [Layer 3](http://searchunifiedcommunications.techtarget.com/definition/layer-3) (IP), via a router. A VLAN abstracts the idea of the LAN; A VLAN might comprise a subset of the ports on a single switch or subsets of ports on multiple switches. By default, systems on one VLAN don't see the traffic associated with systems on other VLANs on the same network. It allows network administrators to [partition](http://searchstorage.techtarget.com/definition/partition) their networks to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure.

There are two major standards in use today :

* Cisco (one of the world's largest network equipment providers) created ISL, or [Inter-Switch Link](https://vlan.wikispaces.com/Definitions). ISL encapsulates frames with the information necessary for trunking. Since ISL is proprietary, its usage is limited to Cisco-only networks.
* IEEE 802.1Q. This vendor-agnostic protocol uses the tagging method to identify the VLAN of the frame. Since this protocol is non-proprietary it has wider device support. Since Cisco gear is expensive, price-sensitive companies frequently opt for affordable (aka !Cisco) gear at the edge. For this reason, the chance of encountering 802.1Q usage in a VLAN environment is very likely. Cisco also supports 802.1Q, so the presence of a Cisco device does not mandate an ISL environment at the expense of 802.1Q.

Routing between VLANs :

The primary advantage of VLANs is that it allows hardware to be consolidated. Before VLANs each broadcast domain requires its own switches to remain separated. The ability to run multiple broadcast domains on the same device as well as share links to other parts of the network allows for cost reduction through economies of scale. This efficiency is offset somewhat by the cost of connectivity. A flat network only needs one gateway to provide outside connectivity. A VLAN network needs a gateway assigned for each VLAN, to communicate with outside networks and each other. Router interfaces are more expensive than switches, but network vendors have developed solutions to reduce costs. Some routers are VLAN aware, and can be trunked directly to a switch. VLANs can have connectivity via subinterfaces, for only the cost of a single router port (and the cost differential of a VLAN-capable switch). This configuration is called a "router on a stick."

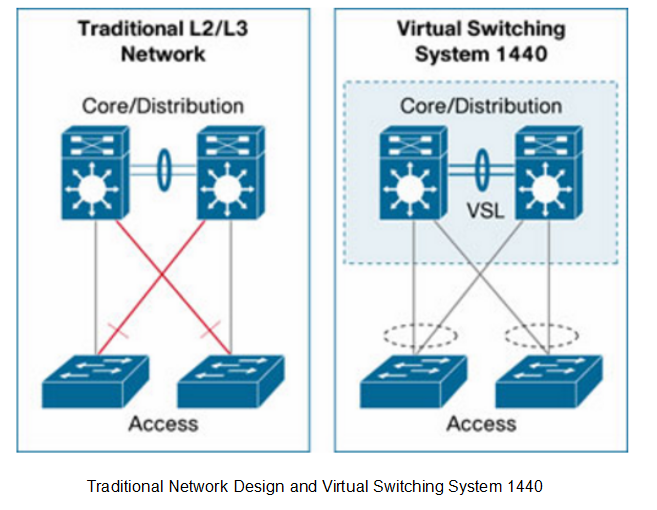
### 3.1.2. Advantages of VLAN

* Flexibility : at the allocation from nodes to network segments, independent from the physical location.
* Easy Management : it is easy to configure large networks using VLAN technology even if the networks are spread across large geographic distances, an administrator is able to manage the entire global network from a single location where the main switching is done. Additionally it requires very little overhead if using a VLAN based on ports which reduces the managerial burden even more for some networks.
* Physical Layer Independence : VLANs are independent on the physical topology and medium over which the network is connected. It is possible to use VLAN technology over a network consisting even of different physical mediums and on the user level this will be completely transparent. In addition the network can span across a large physical distance and even go through an ATM cloud while staying transparent to the users of the same VLAN which could be located across different countries around the globe.
* Security : VLANs provide holistic security to the network by delivering the frames only within the destined VLANs when sending broadcasts and to the specific recipient. This makes it much harder to sniff the traffic across the [switch](https://vlan.wikispaces.com/Definitions) as it will require to both sniff the specific port and not just any port - which allows for extra security. Furthermore when dividing user by VLANs it is possible to make the division according to some security policy and offer sensitive data only to users on a given VLAN without exposing the information to the entire network. Switched network are watched as unsafe because there exists a lot of attack possibilities such as ARP-Spoofing. Routing, which is the only communication possibility between VLANs, is immune to such layer-2-attacks. Moreover routing offers the opportunity to use firewalls, whereby the security becomes increased.
* Cost : Using a network switching with VLANs is cheaper than creating a routed network with expensive routers (routers cost a lot more then switches in general).

## 3.2. Distributed layer : VSS

### 3.2.1. Principle

VSS (Virtual Switching System) is a technology of network system virtualization which combines two Cisco Catalyst 6500 Series switches into a single virtual switch to increase operational efficiency, uninterrupted communications, and extend system bandwidth capacity to 1.4Tbps. Initially, VSS will operate two physical Cisco Catalyst 6500 Series switches as a single logical virtual switch called the Virtual Switching System 1440 (VSS 1440).



### 3.2.2 Advantages

* VSS improves operational efficiency by simplifying networking, reducing switch management overhead by at least 50%.
* VSS optimizes uninterrupted communication. With VSS, L2 / L3 protocol convergence is no longer required in the event of a virtual switch member failure, enabling deterministic virtual switch recovery in one second.
* VSS can expand system bandwidth capacity to 1.4 Tbps. Activate all available L2 bandwidth on redundant Cisco Catalyst 6500 Series Switches to provide automated, accurate load balancing. Its link load balancing is optimized because it is based on more accurate information such as L2 / L3 / L4 parameters and is not the same as VLAN-based load balancing in Spanning-Tree Protocol configuration.

## 3.3 MSTP+VRRP

### 3.3.1. MSTP

The MSTP (Multiple Spanning Tree Protocol) and algorithm provides both simple and full connectivity assigned to any given VLAN through a Bridged Local Area Network. MSTP uses BPDUs (Bridge Protocol Data Unit) to exchange information between spanning-tree compatible devices to prevent loops in each MSTI and in the CIST (Common and Internal Spanning Tree), by selecting active and blocked paths. This is done as well as in STP without the need of manually enabling backup links and getting rid of bridge loops danger. Moreover, MSTP allows frames/packets assigned to different VLANs to follow separate paths, each based on an independent MSTI, within MST Regions composed of LANs and MST Bridges. These Regions and the other Bridges and LANs are connected into a single Common Spanning Tree

### 3.3.2. MSTP Advantages

For fixed bandwidth services, MSTP devices integrate excellent bearer and scheduling capabilities from SDH (Synchronous Digital Hierarchy). For variable bandwidth services, MSTP devices can directly provide end-to-end transparent transmission channels to fully guarantee service quality and make full use of MSTP’s Layer 2 switching and statistical multiplexing share bandwidth and save costs, while using one of the VLAN partitioning capabilities to isolate data and guarantee the quality of service to key users with different levels of quality of service (QoS).

Depending on the requirement of network capacity, we can select the MSTP device in different rates.

### 3.3.3. VRRP

The Virtual Router Redundancy Protocol (VRRP) is a networking protocol that provides for automatic assignment of available IP routers to participating hosts. The protocol achieves this by creation of virtual routers, which are an abstract representation of multiple routers. The default gateway of a participating host is assigned to the virtual router instead of a physical router. VRRP provides information on the state of a router, each VRRP instance is limited, in scope to a single subnet. It doesn’t advertise IP routes beyond that subnet or affect the routing table in any way. VRRP can be used in Ethernet, MPLS and token ring networks with IPv4 as well as IPv6. Because of the GNS3 could not run the VSS, so we chose to use the VRRP in our realization.

### 3.3.4. VRRP Advantages

We can obtain a more reliable default route without change the networking nor configure any dynamic routing or route discovery protocol.

Small network overhead.VRRP defines only one type of packet, a VRRP advertisement packet, and only the router in the master state can send VRRP packets.

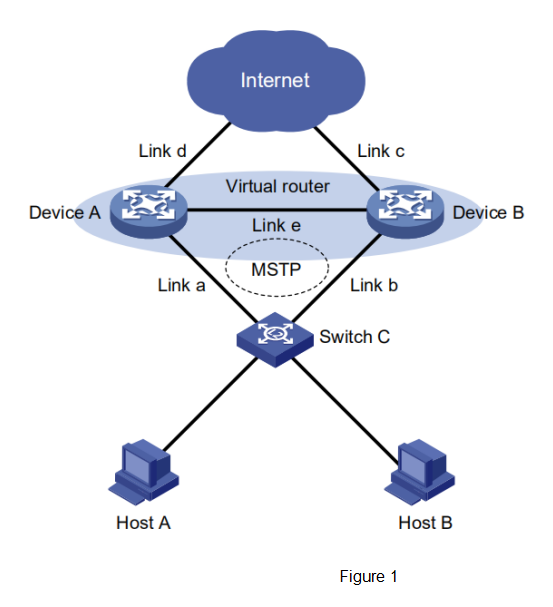
### **3.3.5. VRRP work with MSTP**

VRRP works with MSTP can improve the network reliability

AS the figure 1 shows the networking for using VRRP with MSTP. Add a heartbeat line between Device A and Device B (link e) to provide redundant backup for the downlink and use MSTP to block the network Redundant links to eliminate Layer 2 loops. Adopting to this kind of networking mode, it can not only provide redundant backup for gateway equipment, but also can provide redundant backup for downlink Layer 2 links, which greatly improves the reliability of the network. The networking mode used by VRRP and MSTP has the following advantages:

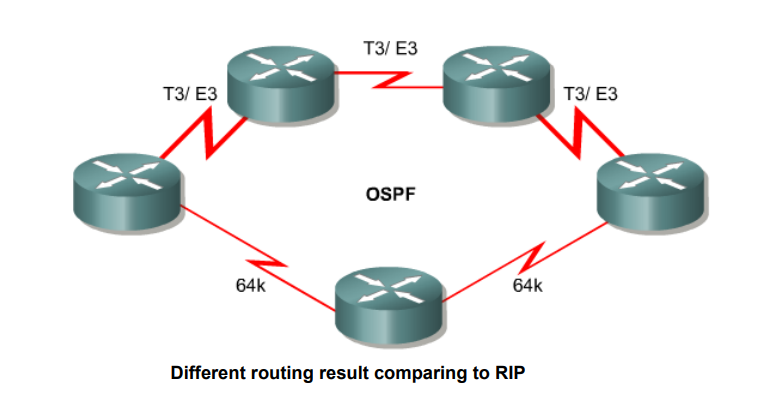
- Protects against multiple link failures. As long as there is one reachable link in the uplink (link c and link d) and one link in downlink (link a and link b), the communication will not be interrupted.For example, if Device A is the master, if link a and link c fail at the same time, traffic will be forwarded through link b-link e-link d. If link a and link d both fail VRRP monitors the uplink interface or link function to reduce the priority of Device A so that Device B becomes the master and traffic is forwarded through link b-link c. If link a and link e fail at the same time, Device B can not receive the Advertisement message of Device A so that Device B becomes the master and traffic is forwarded through link b-Link c.

- We can avoid link a or link b failure or avoid the gateway is working incorrectly for Master and Backup state switching by adding a heartbeat line between Device A and Device B.



## 3.4 Core Layer: OSPF

### 3.4.1 OSPF Routing Protocols

******

Open Shortest Path First (OSPF) is a routing protocol that was created in the mid-1980s because the Routing Information Protocol (RIP) was increasingly incapable of serving large heterogeneous networks. The characteristics below are the reason for choosing OSPF as our routing protocol.

OSPF has two main characteristics. The first one is that it is open which means it’s specification is in the public domain and the second one is that it is based on the SPF or Dijkstra algorithm.

OSPF is a link-state routing protocol that calls for the sending of link-state advertisements (LSAs) to all other routers within the same hierarchical area. Information on attached interfaces, metrics used, and other variables is included in OSPF LSAs. As OSPF routers accumulate link-state information, they use the SPF algorithm to calculate the shortest path to each node.

Large OSPF networks use a hierarchical design. The network is divided into ‘areas’ so as to reduce routing overhead, speed up convergence, confine network instability to an area and generally improve performance. One of the requirements when using the OSPF protocol is that one area, ‘Area 0’ must be defined as the backbone area. It is called the backbone area because all inter-area communication must go through it. All areas should be physically connected to Area 0 so that the routing information injected into this backbone can be disseminated to other areas. The metric used to determine the shortest path to the next router is known as the cost. The cost is the value assigned to a router interface or link and this value is based on the bandwidth of the link. The formula used to calculate it is, cost= 100 000 000/bandwidth in bps (bits per second).

The Link-State is the status of the connection between the two routers (i.e. up or down), and also the relationship between the two routers. Each area is considered as an independent network hence the link-state table only concerns the routers inside that link. Routers use ‘hello’ messages to discover their neighbours and build their topological database for that area. When the state of a link changes, an LSA update is sent to all routers which have to then recalculate their routes.

As stated earlier, OSPF manages larger networks better than the RIP protocol because it is able to divide a network into smaller manageable areas. LSA updates are however processor intensive and a failure or two on a very large network could result in a network going down because there will be too many LSA updates to be processed the network routers. To avoid this, a Designated Router (DR) and Backup Designated Router (BDR) are elected in each local area network to represent that entire network. All LSAs are then sent to the DR and BDR instead of every single router and this greatly reduces the overhead of the LSA updates. The BDR is the redundancy router in the event that the DR goes down. To choose a DR for each network, an OSPF priority number is assigned to each router and the router with the highest number is the DR and the second highest is the BDR. By default all routers have an OSPF priority number of 1.

### 3.4.2 FIREWALL

The ASA in Cisco ASA stands for Adaptive Security Appliance. In brief, Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. It provides proactive threat defense that stops attacks before they spread through the network.

Packet filtering rules can be configured to allow or deny traffic based on variables such as source port, destination port, protocol type, source ip address and destination ip address.

Stateful packet inspection uses the same fundamental packet screening technique that packet filtering does. In addition it examines packet header information from the network layer of the OSI model to the application layer to verify that the packet is part of a legitimate connection and the protocols are behaving as expected. As packets pass through the firewall, packet header information is examined and fed into a dynamic state table where it is stored. The packets are compared to pre-configured rules or filters and ‘allow’ or ‘deny’ are made based on the results of the comparison. The data in the state table is then used to evaluate subsequent packets to verify that they are part of the same connection. The connection state is derived from information gathered in previous packets and is an essential factor in deciding on new communication attempts. Stateful packet inspection compares the packets against the rules and then checks the dynamic state table to verify that packets are part of a valid established connection. By having the ability to remember the status of a connection, this method of packet inspection is better equipped to guard against attacks than standard packet filtering.

An application gateway/proxy can see all aspects of the application layer so it can look for more specific pieces of information. For example, it is able to know the difference between an email containing media and one containing just text. From a security point of view the application gateway/proxy screening method is more superior to other types of packet filtering. This method however is not always an efficient use of the network because it can seriously impact performance since all incoming and outgoing traffic is inspected at the application level. This impacts scalability of such a network. Another disadvantage is that each protocol requires its own proxy application. If one does not exist then the corresponding protocol will not be allowed through the firewall. This makes support for new protocols challenging. Other disadvantages include high implementation cost and additional client configuration.

### 3.4.3 NAT

NAT is a mechanism of translating a IP private address to a IP public address. NAT is a process used to translate network addresses. NAT’s primary use is to conserve public IPv4 addresses. NAT is usually implemented at border network devices, such as firewalls or routers. NAT allows the networks to use private addresses internally, only translating to public addresses when needed. Devices within the organization can be assigned private addresses and operate with locally unique addresses. When traffic must be sent or received to or from other organizations or the Internet, the border router translates the addresses to a public and globally unique address. To enable access to a lower level interface from a higher level interface use the nat and global commands.

Inside network is the set of devices using private addresses Outside network refers to all other networks. NAT includes four types of addresses:

* Inside local address
* Inside global address
* Outside local address
* Outside global address

### 3.4.4 Static NAT

Static NAT uses a one-to-one mapping of local and global addresses. These mappings are configured by the network administrator and remain constant. Static NAT is particularly useful when servers hosted in the inside network must be accessible from the outside network. A network administrator can SSH to a server in the inside network by pointing the SSH client to the proper inside global address.

### 3.4.5 Dynamic NAT

Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool. Dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.

Some of the benefits are-

Conserves the legally registered addressing scheme , increases the flexibility of connections to the public network , provides consistency for internal network addressing schemes and provides network security

The enterprise has connection to Internet using another router. The router NAT, it is used for doing internal routing.

### 3.4.5 ACL

Along with firewalls, ACLs are also going to be used to filter incoming and outgoing packets.

Packet filtering, sometimes called static packet filtering, controls access to a network by analyzing the incoming and outgoing packets and passing or dropping them based on given criteria, such as the source IP address, destination IP addresses, and the protocol carried within the packet. A router acts as a packet filter when it forwards or denies packets according to filtering rules. An ACL is a sequential list of permit or deny statements, known as access control entries (ACEs).

The last statement of an ACL is always an implicit deny. This statement is automatically inserted at the end of each ACL even though it is not physically present. The implicit deny blocks all traffic. Because of this implicit deny, an ACL that does not have at least one permit statement will block all traffic.

Wildcard masks and subnet masks differ in the way they match binary 1s and 0s. Wildcard masks use the following rules to match binary 1s and 0s: Wildcard mask bit 0 - Match the corresponding bit value in the address. Wildcard mask bit 1 - Ignore the corresponding bit value in the address. Wildcard masks are often referred to as an inverse mask. The reason is that, unlike a subnet mask in which binary 1 is equal to a match and binary 0 is not a match, in a wildcard mask the reverse is true.

Use ACLs in firewall routers positioned between your internal network and an external network such as the Internet. Use ACLs on a router positioned between two parts of your network to control traffic entering or exiting a specific part of your internal network. Configure ACLs on border routers, that is routers situated at the edges of your networks. Configure ACLs for each network protocol configured on the border router interfaces.

The Three P’s –

One ACL per protocol - To control traffic flow on an interface, an ACL must be defined for each protocol enabled on the interface.

One ACL per direction - ACLs control traffic in one direction at a time on an interface. Two separate ACLs must be created to control inbound and outbound traffic.

One ACL per interface - ACLs control traffic for an interface, for example, GigabitEthernet 0/0.

Every ACL should be placed where it has the greatest impact on efficiency. The basic rules are:

Extended ACLs - Locate extended ACLs as close as possible to the source of the traffic to be filtered.

Standard ACLs - Because standard ACLs do not specify destination addresses, place them as close to the destination as possible.

Placement of the ACL and therefore the type of ACL used may also depend on: the extent of the network administrator’s control, bandwidth of the networks involved, and ease of configuration.

### 3.4.6 DMZ

DMZs, also known as perimeter networks are a network region separate from the private internal network but access is still restricted from the external world. They are created to give untrusted users access to required data while minimizing the risk to the internal network.

Perimeter Network with Back-To-Back Firewalls: It requires two Firewalls. Web or Server Publishing is used to allow perimeter network servers to access servers on the internal network.

Cisco ASA 5500 series is a solution that integrates firewall, unified communications security,SSL, IPsec VPN, intrusion prevention and content security. It delivers content security services: URL Filtering, Anti-phishing, Anti-spam, Antivirus and content filtering - which can help lower operation costs, reduce liability and improve employee productivity.

The Network can be divided based on the levels of security that is assigned to them. For example the outside network has a default value of 0 whereas the inside level has a security value of 100 and the DMZ have a security value of 50. Security levels let you control access between systems on different interfaces and the way you enable or restrict access depends on the security level of the interfaces. Different methods have to be implemented in order to allow traffic among the different layers of security.

- ACL’s are used in order to enable access to a higher security level interface from a lower security level interface.

- NAT is implemented in order to enable access to a lower level interface from a higher level interface.

## 3.5 SERVER

### 3.5.1 LDAP

******

Lightweight Directory Access Protocol(LDAP) is a protocol based on X.500 standard. Though it's based on the x.500 standard, but it's much simpler and can be customized as needed. Unlike x.500, LDAP supports TCP/IP, which is necessary to access the Internet. The LDAP directory stores data in a tree-like hierarchy.

LDAP is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

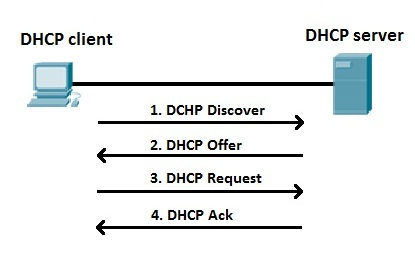
It is a simplification of the Directory Access Protocol (DAP) used to access directory information. A directory is essentially a special-purpose database optimized to handle identity-related information. The LDAP standard also defines a data model based on the X.500 data model. It is a hierarchical data model, with objects arranged in a hierarchical structure, and each object containing a collection of attributes. The overall structure of any particular directory is defined by its schema, much like a database schema defines the tables and columns.

LDAP defines a “Bind” operation that authenticates the LDAP connection and establishes a security context for subsequent operations on that connection. There are two authentication methods defined in RFC 4513, simple and SASL. The simple authentication method has the LDAP client send the username (as a LDAP distinguished name) and password (in clear text) to the LDAP server. The LDAP server looks up the object with that username in the directory, compares the password provided to the passwords stored with the object, and authenticates the connection if they match. Because the password is provided in clear text, LDAP simple Binds should only be done over a secure TLS connection.

SASL Bind is more involved, and allows the client and server to negotiate a particular authentication mechanism, which they then use to authentication the LDAP connection.

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically. An LDAP server is called a Directory System Agent (DSA). An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSAs as necessary, but ensuring a single coordinated response for the user.

### 3.5.2 DHCP

******

Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks. The DHCP is controlled by a DHCP server that dynamically distributes network configuration parameters, such as IP addresses, for interfaces and services. DHCP server enables computers to request IP addresses and networking parameters automatically, reducing the need for a network administrator or a user to configure these settings manually.

DHCP provides an automated way to distribute and update IP addresses and other configuration information on a network. A DHCP server provides this information to a DHCP client through the exchange of a series of messages, known as the DHCP conversation or the DHCP transaction. If the DHCP server and DHCP clients are located on different subnets, a DHCP relay agent is used to facilitate the conversation.

1. When a client connects to a network, it sends a discover message to the server, containing the source ip and subnet mask.

2. The server then replies with a discover message that contains all required info for the network configuration of the client. Usually ip to be assigned to client, subnet mask and default gateway

3. The client sends another message/ request acknowledging receipt and acceptance of the configuration in the offer it received.

4. If the request was sent to multiple dhcp servers, the client receives multiple offers, but accepts only one of them by populating the server field with the ip address of a particular DHCP server. All other offers is declined.

5. When the server receives this new request from the client, it sends another message indicating that the client can now use the IP it assigned to it.

6. This ip address assigned by DHCP server are usually on lease.

7. After the lease expires, the server may assign them to a different client

8. DHCP clients try to renew this lease after half of the lease time has expired. This is also known as renewing stage.

We will use a “help address” when the server DHCP isnot directly connected. This is used in case our router just drops down.

### 3.5.3 DNS

The Domain Name System (aka DNS) is used to resolve human-readable hostnames into machine-readable IP addresses. DNS also provides other information about domain names, such as mail services.

DNS is like a phone book for the Internet. If you know a person’s name but don’t know their telephone number, you can simply look it up in a phone book. DNS provides this same service to the Internet.

It involves following steps ：

Step 1: Request information

The process begins when we ask to resolve a hostname we are visiting. The first place it looks is its local DNS cache, which stores information that your computer has recently retrieved. It needs to perform a DNS query to find out if not already available.

Step 2: Ask the recursive DNS servers

If the information is not stored locally, your computer queries (contacts) the ISP’s recursive DNS servers. These specialized computers perform the legwork of a DNS query on our behalf. Recursive servers have their own caches, so the process usually ends here and the information is returned to the user.

Step 3: Ask the root nameservers

If the recursive servers don’t have the answer, they query the root nameservers. A nameserver is a computer that answers questions about domain names, such as IP addresses. The thirteen root name servers act as a kind of telephone switchboard for DNS. They don’t know the answer, but they can direct our query to someone that knows where to find it.

Step 4: Ask the TLD nameservers

The root name servers will look at the first part of our request, reading from right to left — www.hostname.com — and direct our query to the Top-Level Domain (TLD) nameservers for .com. Each TLD, such as .com, .org, and .us, have their own set of nameservers, which act like a receptionist for each TLD. These servers don’t have the information we need, but they can refer us directly to the servers that do have the information.

Step 5: Ask the authoritative DNS servers

The TLD name servers review the next part of our request — *www.hostname.com* — and direct our query to the nameservers responsible for this *specific* domain. These authoritative nameservers are responsible for knowing all the information about a specific domain, which are stored in DNS records. There are many types of records, which each contain a different kind of information. In this example, we want to know the IP address for *www.hostname.com*, so we ask the authoritative nameserver for the Address Record (A).

Step 6: Retrieve the record

The recursive server retrieves the A record for hostname.com from the authoritative nameservers and stores the record in its local cache. If anyone else requests the host record for hostname.com, the recursive servers will already have the answer and will not need to go through the lookup process again. All records have a time-to-live value, which is like an expiration date. After a while, the recursive server will need to ask for a new copy of the record to make sure the information doesn’t become out-of-date.

Step 7: Receive the answer

Armed with the answer, recursive server returns the A record back to your computer. Our computer stores the record in its cache, reads the IP address from the record, then passes this information to our browser. The browser then opens a connection to the web server and receives the website.

## 3.6 External network

### 3.6.1 BGP+IS-IS

**Advantages of BGP:**

* Server only need to set up one IP address, the best path is decided by backbone routers according to the hop or other indicators. Will not occupy any server system resources.
* When a line fails, the route will automatically switch to other lines.
* Makes the network has a strong scalability, easy to implement single IP multi-line

Advantages of IS-IS

* **Reliability:** OSPF protocol is based on IP layer, so it can only support IP network, some IP based attacks will affect the operation of OSPF. IS-IS runs directly on the link layer, which can host multiple network types and has some natural advantages in preventing network attacks.
* **Scale:** The IS-IS calculates the route using the PRC calculation. The ip prefix serves as the leaf node of the shortest spanning tree, and OSPF is established around the link. In the same size area, IS-IS is more stable, consumes less resources and supports larger networks.
* **Flexibility:** The OSPF protocol is flexible. The protocol is interface-based. The types of networks it supports are comprehensive, mature and compatible, and can meet the needs of a large number of users with complex routing control
* **Extensibility:** IS-IS is structured, stable and scalable. IS-IS supports multiple network protocols (OSPF only supports IP). IS-IS can smoothly translate, split, merge, and traffic Uninterrupted

### 3.6.2 MPLS VPN

**Definition:**

Multiprotocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks. MPLS directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence its name "multiprotocol". MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL.

MPLS VPN is a family of methods for using multiprotocol label switching (MPLS) to create virtual private networks (VPNs). MPLS VPN is a flexible method to transport and route several types of network traffic using an MPLS backbone.

**Advantages：**

* **QoS:** MPLS VPN is based on the backbone network, with the best quality of service in the network. IPSec VPNs guarantee the security of end-to-end network transport channels. Encryption and decryption at the endpoints require additional hardware and software processing power, which adds to user and performance overhead.
* **Convenience:** MPLS VPN In the MPLS VPN internal network, users are all like in the same network, without installing any client software. IPSec VPN requires a client installation before it can be used.
* **Scalability:** MPLS VPN providers can simply configure the MPLS VPN as a full mesh structure,enterprises only need to connect CE with PE in a variety of ways. Because of the need to traverse the firewall, the IP address Conflict and other issues, IPSec VPN usually can not support complex networks.

# 4. Special functions

## 4.1 IPv6 to IPv4

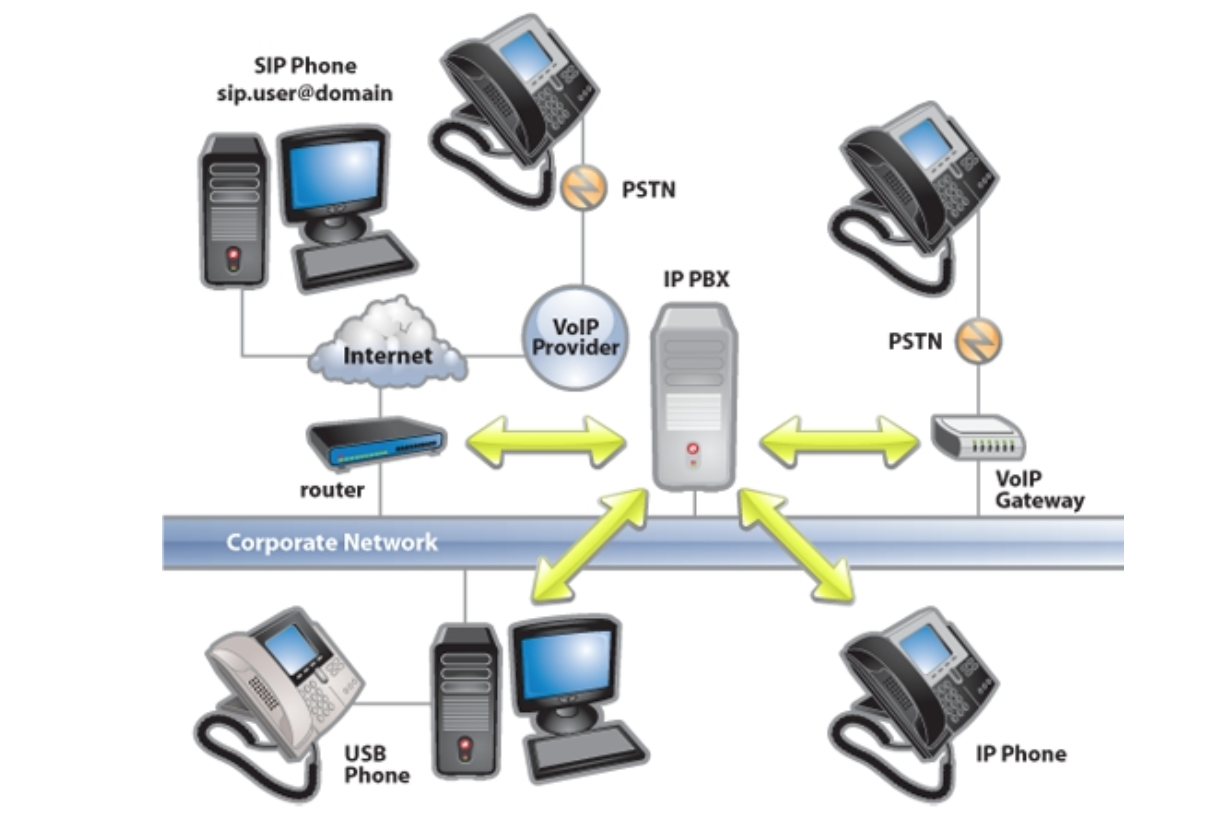
**Solutions：**

* Dual-Stack Network: IPv4 and IPv6 operate in links at the same time, which means hosts should supports both protocols
* Tunneling: Build an overlay network that tunnels one protocol over the other by encapsulating IPv6 packets within IPv4 packets and IPv4 packets within IPv6 packets. (eg. Configured Tunnel, Auto-configured Tunnel, Tunnel Broker, 6 over 4, 6 to 4, BGP Tunnel, MPLS Tunnel)
* Conversion mechanism: Use the transformation gateway to convert between IPv4 and IPv6 networks.(eg. NAT-PT, NAT64)

### 4.1.1 Generale Advantages of tunneling

When IPv6 routing domains are isolated and need to communicate, tunneling mechanisms can allow connectivity across an existing IPv4 network (including the Internet) without widespread configuration issues. In many cases, this is a router-to-router (or gateway) type of deployment, though some mechanisms exist for host-to-host (such as Microsoft Teredo tunneling), or host-to-router. Some tunneling mechanisms require explicit source and destination designations, while others are automated, using embedded addressing to locate the peer device. In most cases, tunneling allows for isolated and/or simplified IPv6 deployment, coining the phrase “dual stack where you can; tunnel where you must”.

## 4.2 VoIP



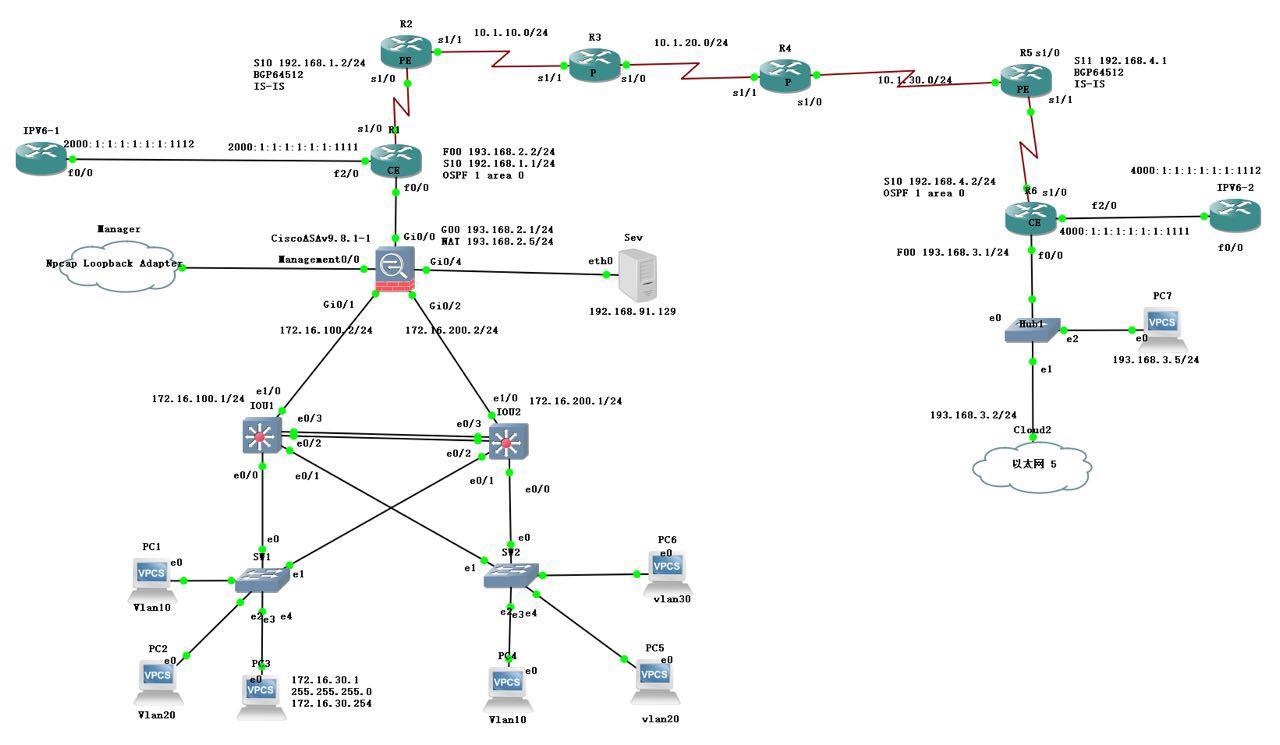
An IP PBX system is what is also known as a VOIP system and delivers voice or video over a data connection. It can also interoperate with the traditional PSTN.

The IP PBX will convert the voice in to data and transfer it across the network as packets. Using data networks for voice can significantly reduce the cost of long distance, and international phone calls; and considerably reduce the overheads of traditional line rentals. Your traditional PBX solution may be able to connect to a data network using a SIP trunk, as nearly 75% of business PBXs are IP enabled.

An IP PBX solution is also able to switch calls between VoIP and traditional telephones while still offering the same functionality of your traditional PBX phone system. It is different from a hosted or cloud based solution as the IP PBX is owned by the business, just as with a traditional PBX.It can exist as a hardware or software-only solution.

# 5.Simulation on GNS3 and VMware

## 5.1 Architecture



* Overview of the design

In the topology, different departments are divided to different vlans. And we use layer 3 switch to achieve the communication between different vlans. To achieve the redundancy and avoid loop, we use MSTP+VRRP in layer 3. Then we use firewall to filter some traffic and achieve the transmission from private addresses to public ones. We also put our servers in DMZ, so that users who doesn't belong to this company can get information from these servers in DMZ, and can't access the network of company. R1 is the edgerouter of company, we set up a VPN between two companies (R1 to R6), it can ensure the security of information during transmission. Besides that, we set up a tunneling for IPv6 to IPv4.

* Technologies used :
  1. Vlan

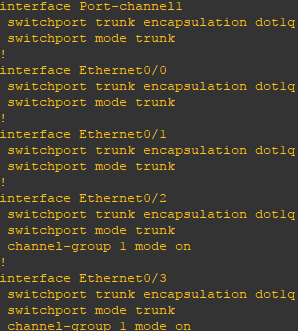
Different departments are divided to different vlans.

Vlan is used to decrease the size of broadcast



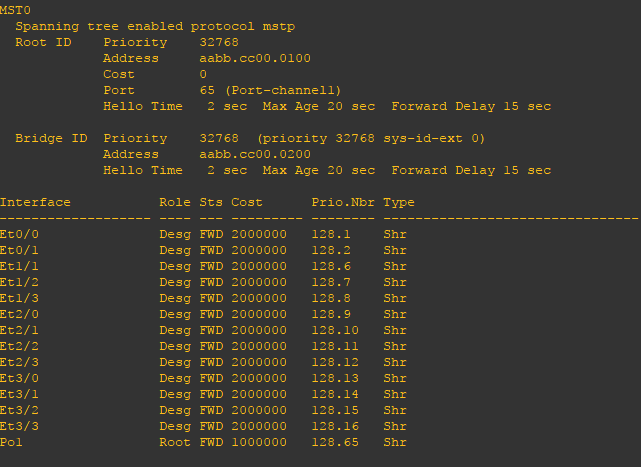
* 1. Trunk

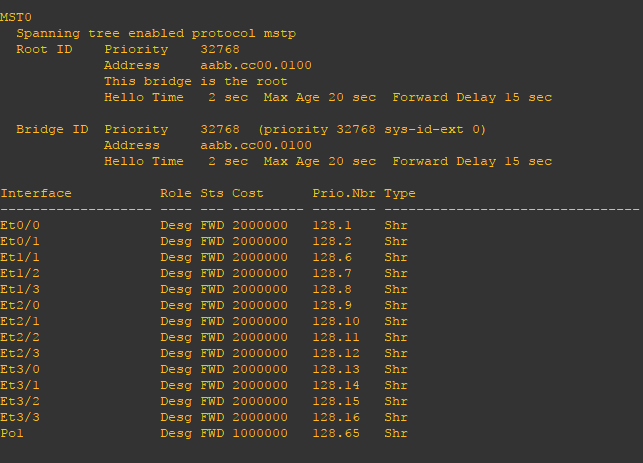
We set Trunk between layer 2 switch (sw1 & sw2) and layer3 (IOU1 & IOU2). It's used to transmit different vlans information in one line.



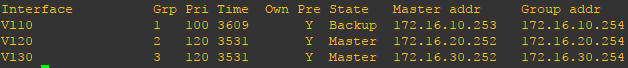
* 1. MSTP+VRRP+EtherChannel

**MSTP**: to avoid loop link



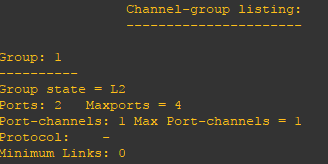


**VRRP**: We use it to assign one layer 3 switch as a master , and another one is backup. When the master one is down , the backup will become the master one immediately to achieve the redundancy of network.



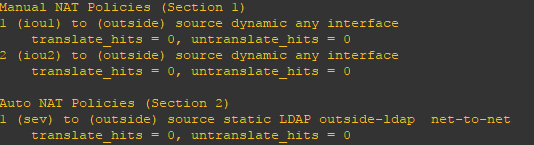


**EtherChannel**: Grouping of several physical Ethernet links to create one logical Ethernet link. It can provide fault-tolerance and high-speed links between two switches.

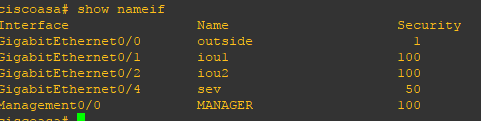


* 1. Firewall

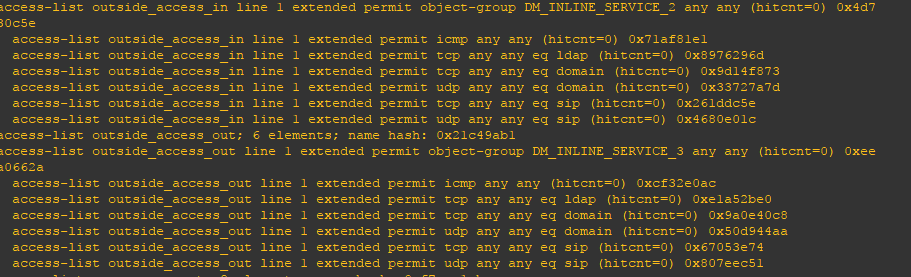
**NAT**: It is used to achieve the transformation of addresses. In our topology, we use two nats. One is used to transfer private addresses into public ones. It makes staff of the company can access the internet. Another one is a map between local servers and public address. Then these customers can access some severs of companies.



**DMZ**: We put servers in this zone, people that don't belong to this company can get some information from our servers, but they can't access the network of company.



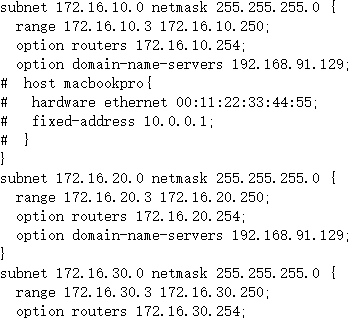
ACL: Allow customers to access servers of our company but prevent all traffic from accessing internal network.



* 1. Servers

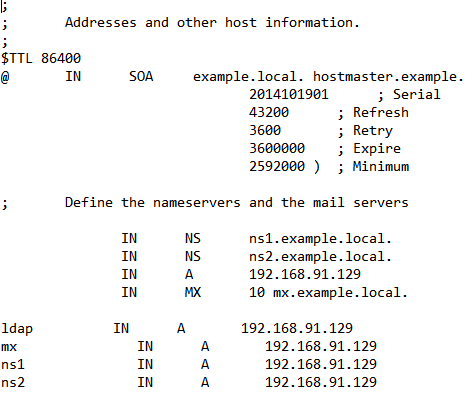
**DHCP server**: Assign ip address and related informations

In this topology, we set up three pools according to three different vlans.



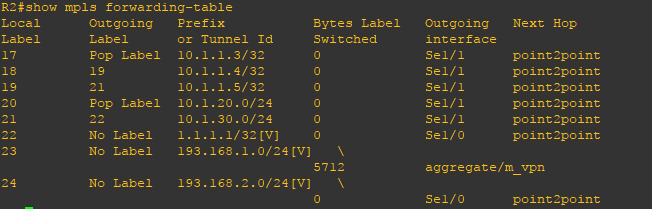
**DNS server**: transfer domain name to ip address

(We have installed **CentOS 7** on VMware and configure DHCP and DNS server on it.)



* 1. **MPLS VPN** （From R1 to R6）

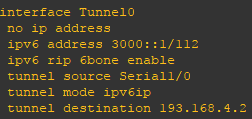
Considering the scale of the company and security, we choose MPLS VPN to achieve the connection with its branch company.



* 1. IPv6 to IPv4

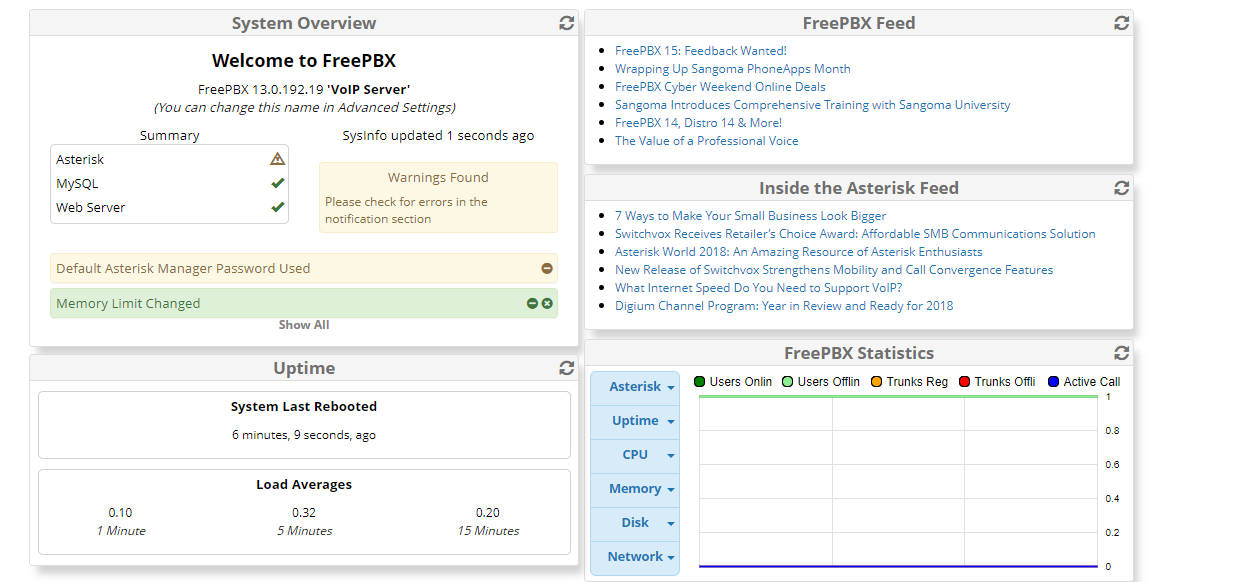
6to4 is the method of choice for users or networks that want to connect to the IPv6 Internet using an IPv4 connection. It allows these users to communicate with other 6to4 users as well as users of native IPv6 connections.





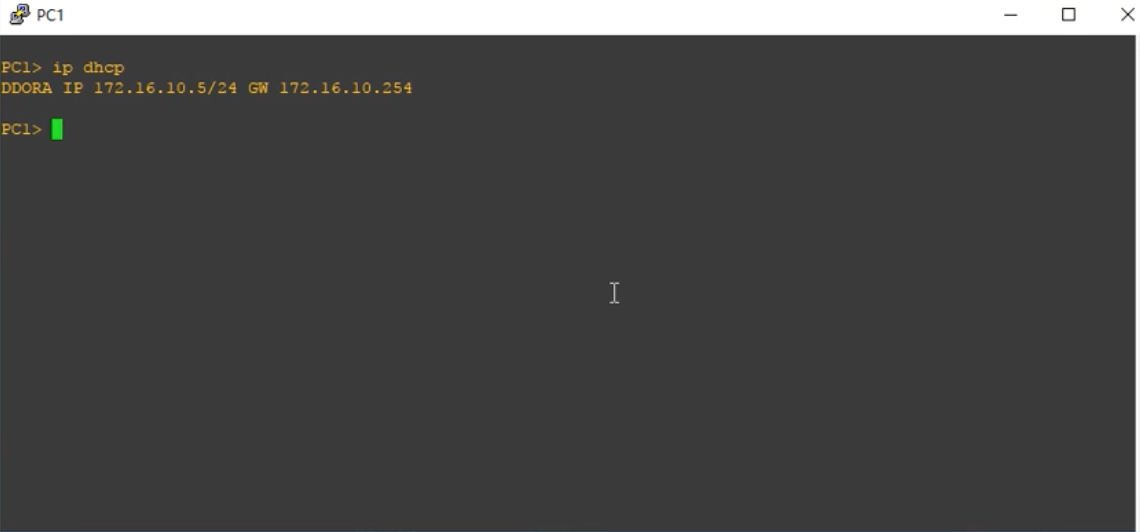
(8)VoIP

A PBX server is configured in this system to achieve communication of IP phone.

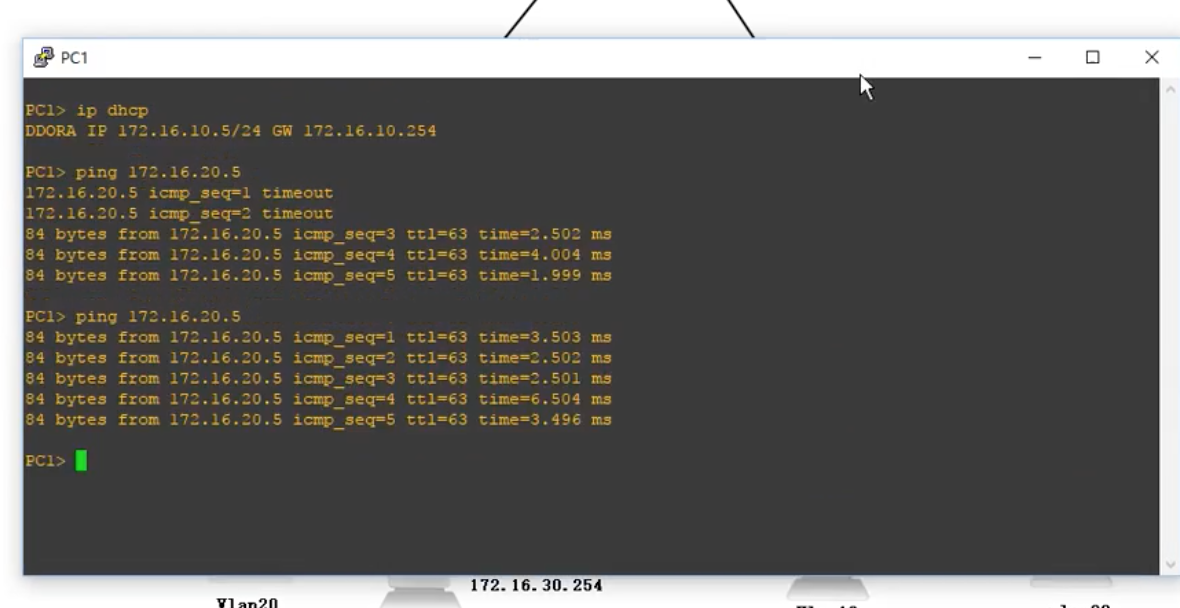


## 5.2 Results

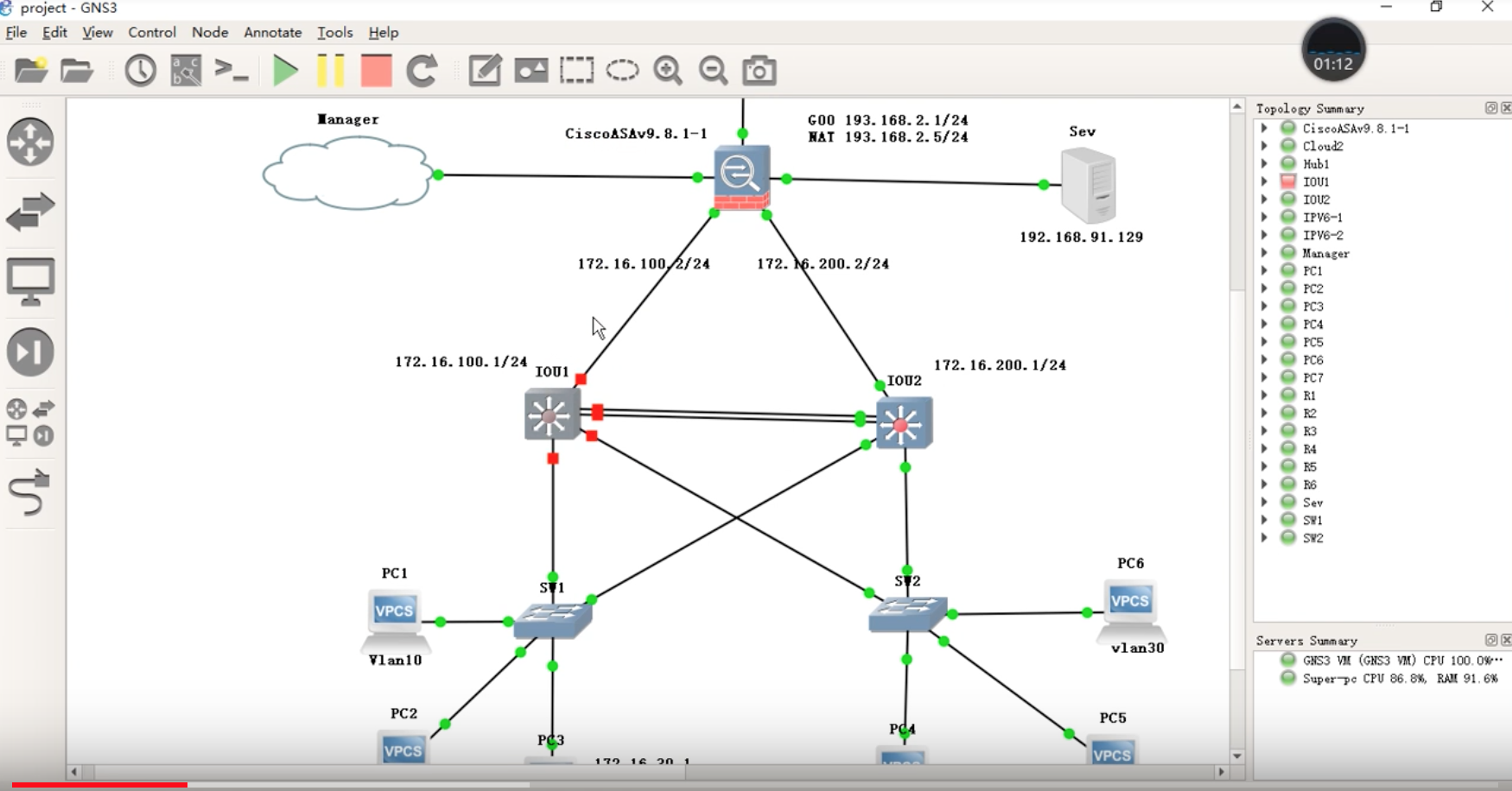
1. DHCP

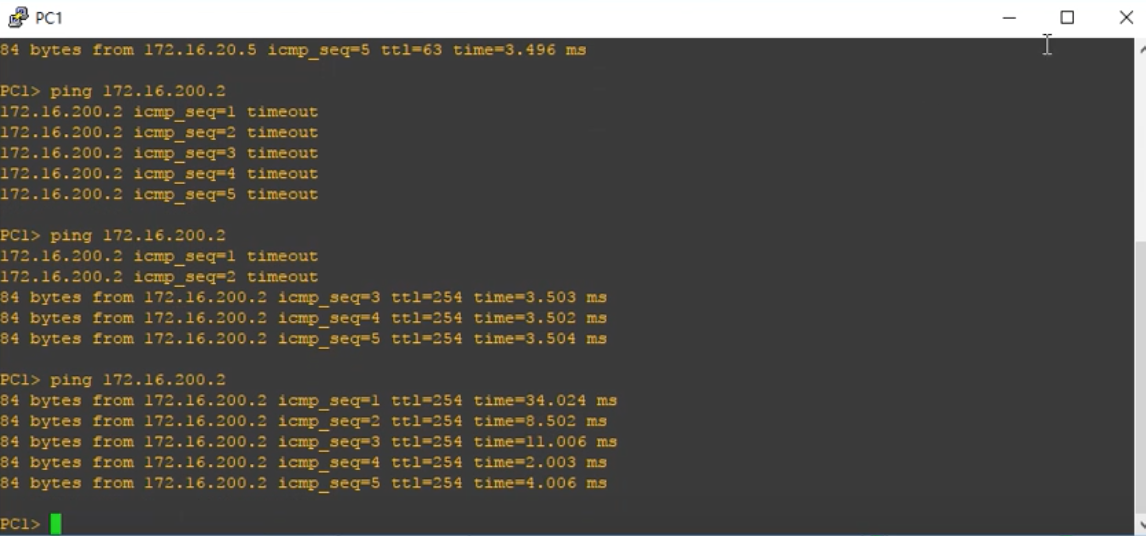


1. VLAN

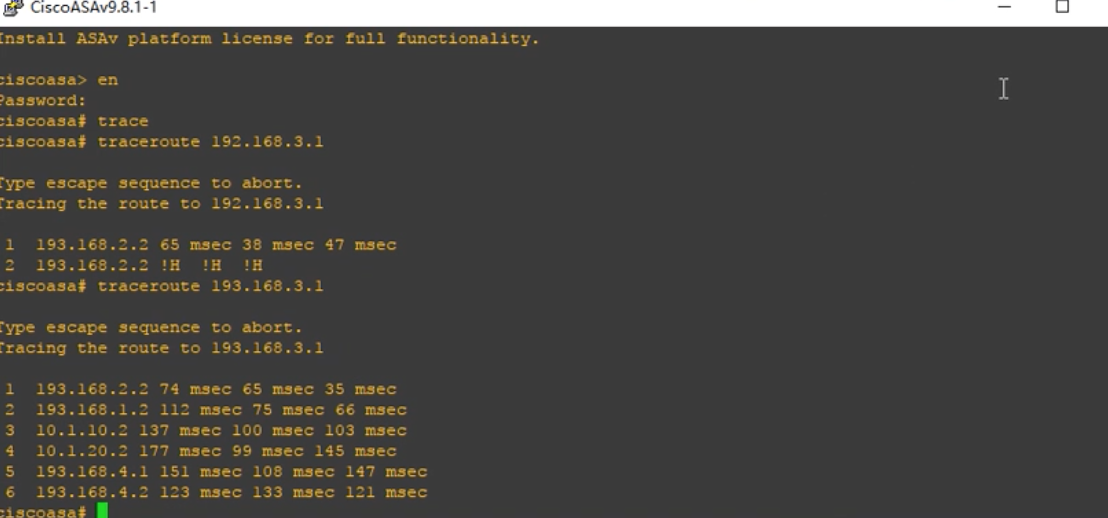


1. VSS

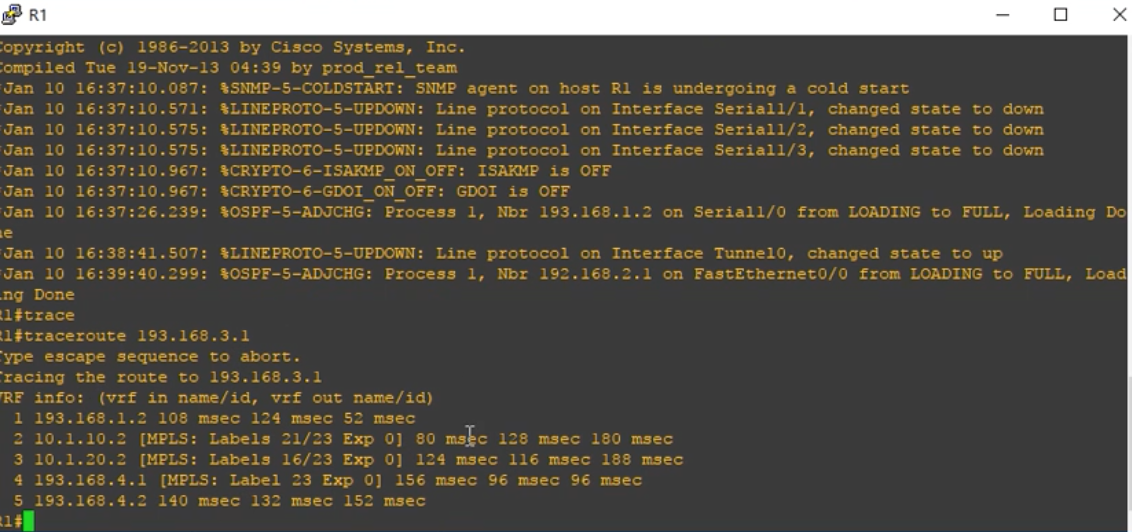




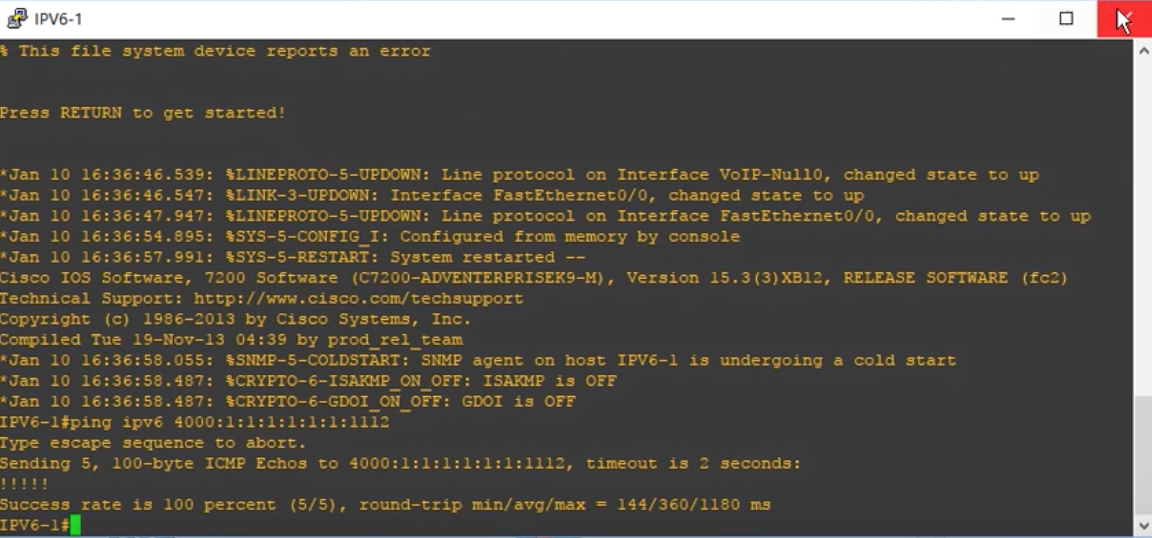
1. NAT

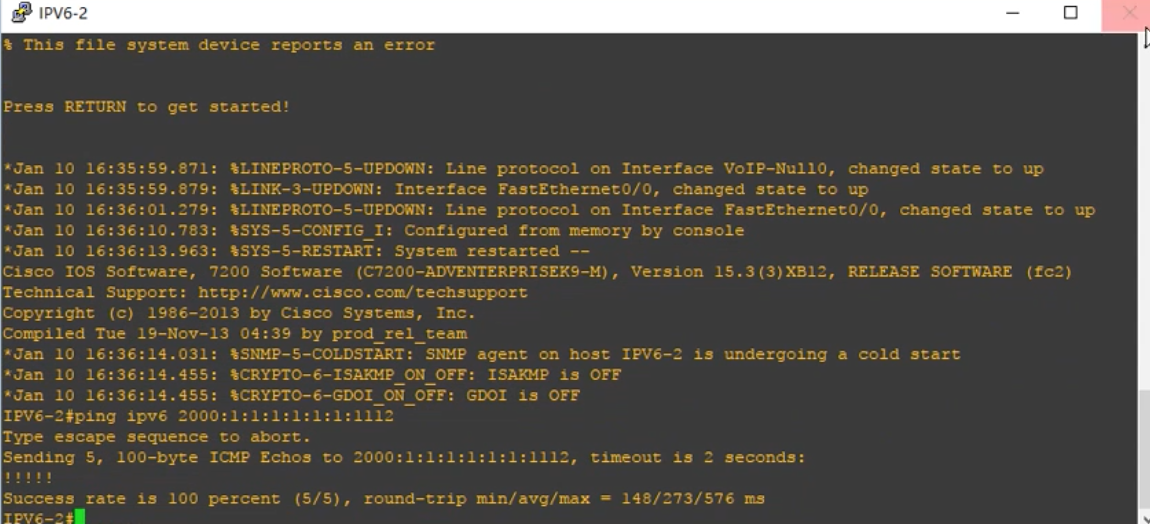


1. MPLS

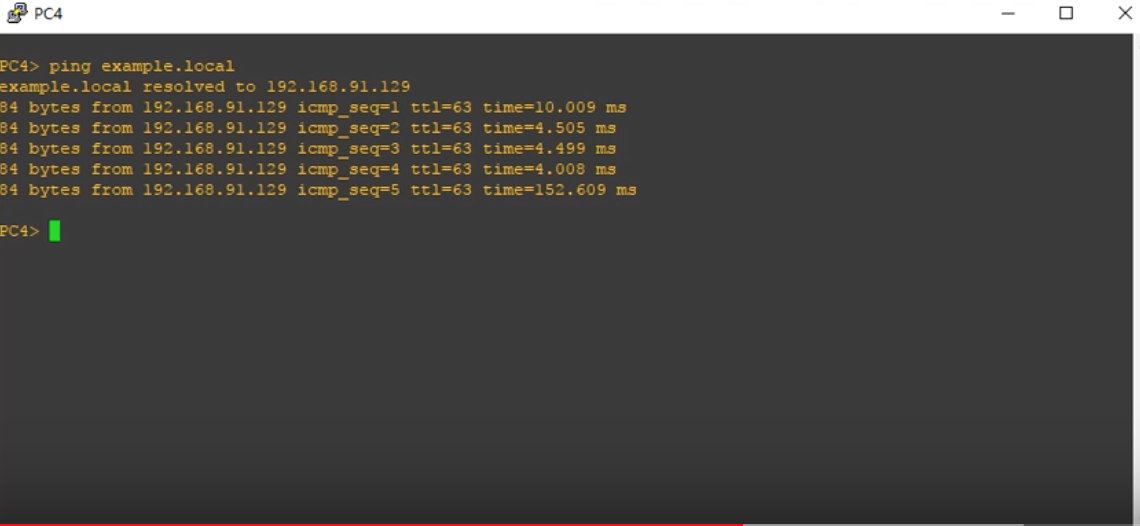


1. IPv6 to IPv4

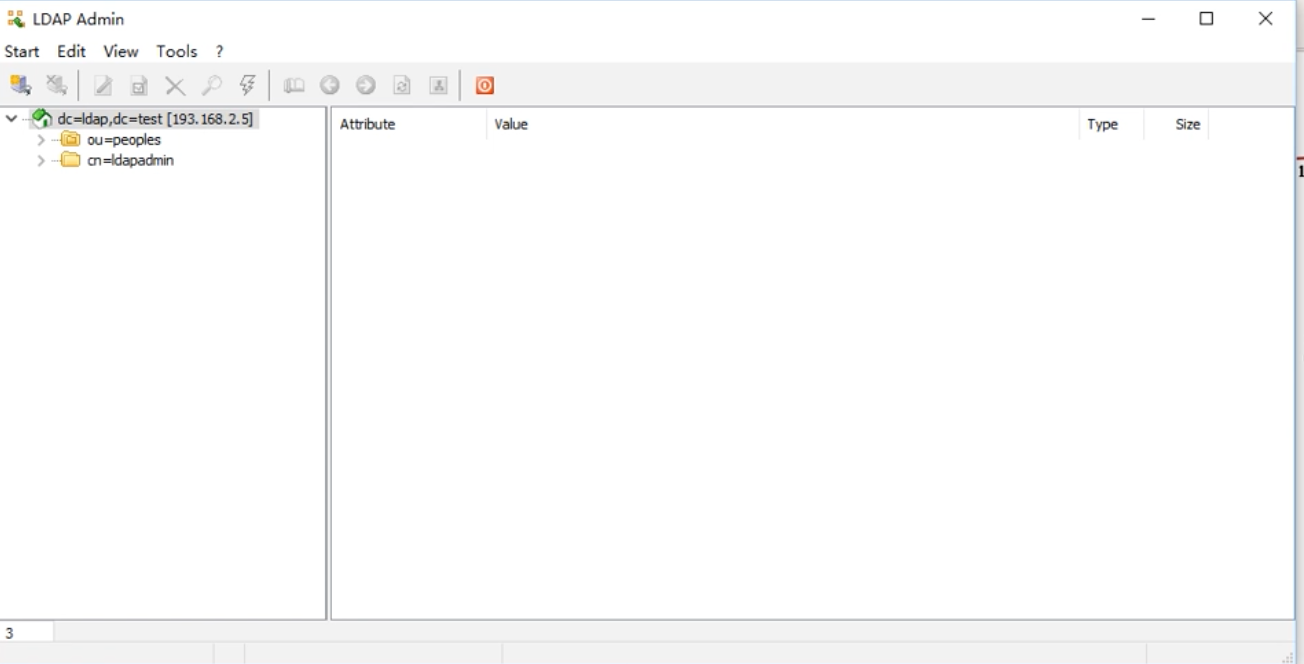




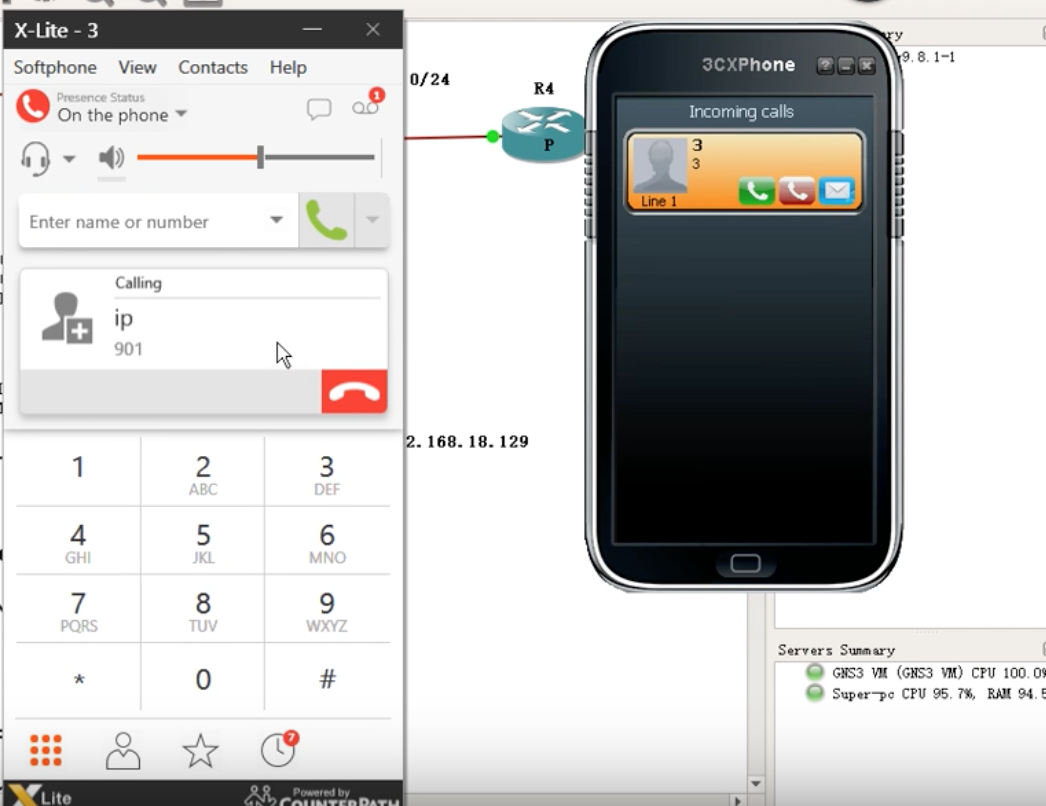
1. DNS



1. LDAP



1. VoIP



# 

# 

# References

1. <https://www.cisco.com/c/zh_cn/products/collateral/switches/catalyst-6500-virtual-switching-system-1440/prod-qas0900aecd806ed74b.html>
2. <https://vlan.wikispaces.com/VLAN+Principles+of+Operation>
3. <http://blog.csdn.net/u013982161/article/details/51192337>
4. <http://denisrosenkranz.com/tuto-installer-et-configurer-openldap-sous-centos/>
5. <https://blog.feehi.com/linux/678.html>
6. <http://blog.topspeedsnail.com/archives/5497>
7. <https://www.cisco.com/c/zh_cn/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html>
8. <http://blog.sina.com.cn/s/blog_53e853840100nis7.html>
9. <https://wenku.baidu.com/view/65a16618cc7931b765ce15e4.html>
10. <http://www.tech-faq.com/understanding-the-cisco-three-layer-hierarchical-model.html>
11. <http://www.dummies.com/programming/networking/cisco/working-with-routing-information-protocol-rip/>
12. <https://educ.isep.fr/moodle/mod/resource/view.php?id=5877>
13. <https://www.quora.com/What-is-LDAP-and-how-does-LDAP-authentication-work>
14. <https://technet.microsoft.com/en-us/library/cc780760(v=ws.10).aspx>
15. <https://educ.isep.fr/moodle/mod/resource/view.php?id=5877>
16. CHEN Zhu，WANG Shuo. Comparison of the advantages and disadvantages of MPLS VPN and IPSec VPN[J]. mobile communication,2016,40(12): 24-28.
17. MA Yan, ZHAO Xiaoyu. Summarization of IPv4 to IPv6 Transition Mechanisms[ J ]. Journal of Beijing University of Posts and Telecommunications,2002,(12): 25-4