Paramount Healthcare

Advanced Computer Networks Project 2019

Contents

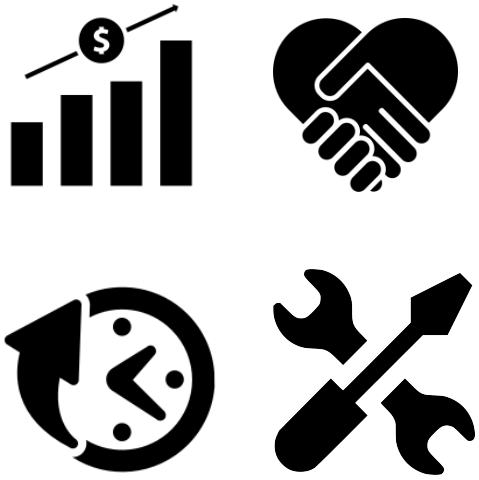
Touchpoint 1

About

- We have been employed to help Paramount Healthcare overcome their networking issues.
- Goal of the project is to get a feel of designing a network in real time.
- We have been given limited amount of information, and as network designers we must make the best use of it and come up with an appropriate network design that meets the needs of paramount healthcare.

Business Goals

- Increase revenue and profit.
- Offer affordable customer services.
- Offer better customer support.
- Modernize outdated technologies.
- Avoid business disruption due to network security problems.
- Reduce telecommunications and network costs.
- More efficient usage of power, cabling, storage, and WAN circuits.



Stuntman - Persona

- Fit and healthy individual
- Makes $5000 - $10000 a year
- Exposed to harsh climates
- Risky profession
- Physical injuries like fractures, cuts, bruises, abrasions and burns
- Can also injure internal organs like spleen, liver and intestine

Doctor - Persona

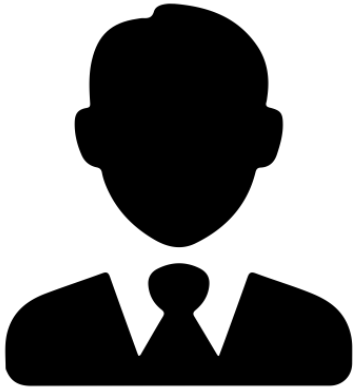
- Makes $40000 - $70000 a year
- Needs access to internet, database and medical imaging software
- Is not concerned about the network design, *it should just work*
- Busy schedule
- Needs to sign documents on a computer
- Needs printer access for patient reports

Nurse - Persona

- Makes $4000 - $10000 a year
- Needs access to internet, database, medical imaging software and servers
- Frequent access to patient records
- Busy schedule
- Needs wireless access point
- Needs printer access for patient reports

Administrator - Persona

- Makes $9000 - $25000 a year
- Needs access to internet, databases and servers
- Secure and exclusive access to DBs
- Handle sensitive data
- Needs wireless access point
- Needs printer access for documents



Scope

We will focus on:

- Medical grade network
- High availability
- Redundancy
- Internet issues

We will *not* focus on:

- Handling external security threats
- Network segmentation
- Handling ISP Failure

Medical Grade Network

A Medical Grade Network is a network designed to handle the needs of a healthcare organization.

- Follows the 3-layer model - Core, Access and Distribution layers
- Handles Clinical Data and Critical Clinical Data
- Structured IP addressing with summarization
- QoS is embedded in infrastructure design
- Redundant devices present in core and distribution layers
- Has High Availability

QoS

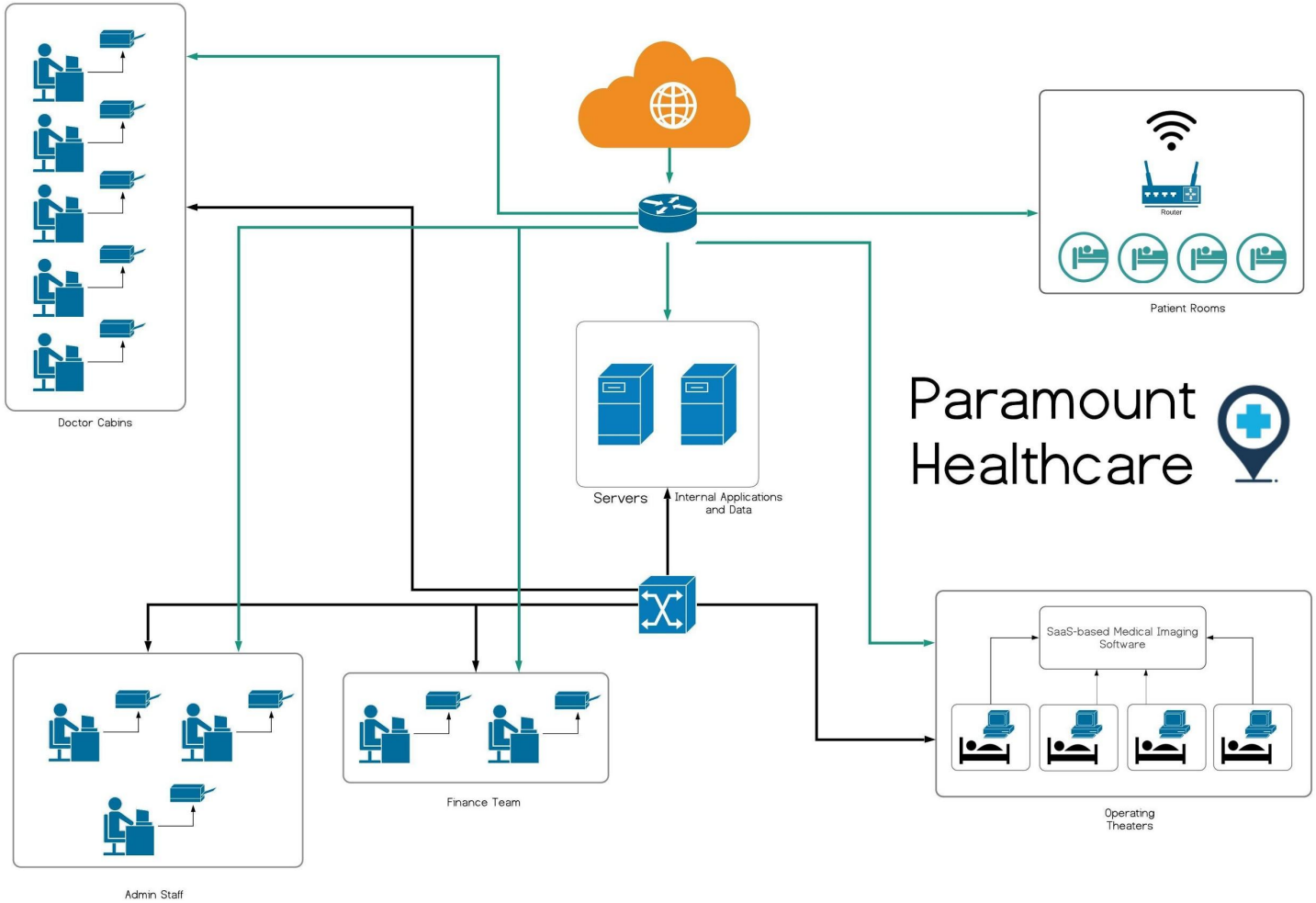
- **Parameters**
  - Jitter - below 30ms
  - Bandwidth - 100 mbps (for OpenMRS and real-time imaging service)
  - 5-nines availability
  - Latency - must not cross 150ms, i.e, RTT <= 300ms

- **Differentiated Services (DiffServ) QoS Model**
  QoS model where network elements, such as routers and switches, are configured to service multiple classes of traffic with different priorities. Network traffic must be divided into classes based on a company's requirements.

Existing Network

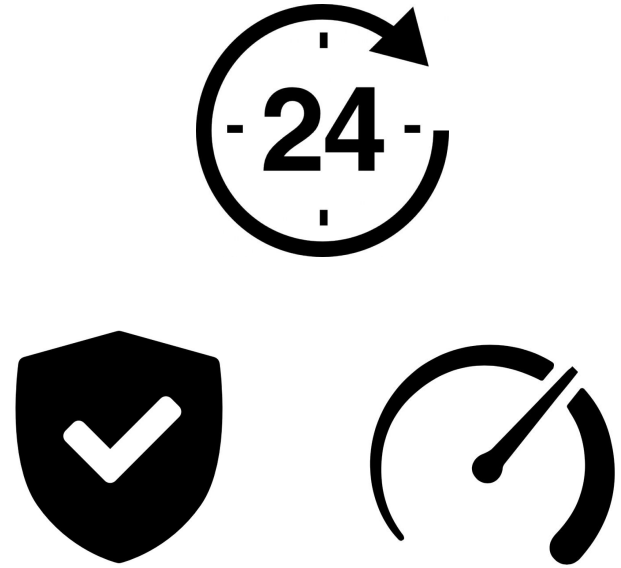
Assumptions

- The organisation was founded in 2015, and it may not have taken scalability in account.
- Slow internet is due to multiple connections to the same router.
- No segmentation of the network.
- Sensitive financial data accessed over common network.
- SaaS based software is accessed over common internet.
- No redundancy present in the network.

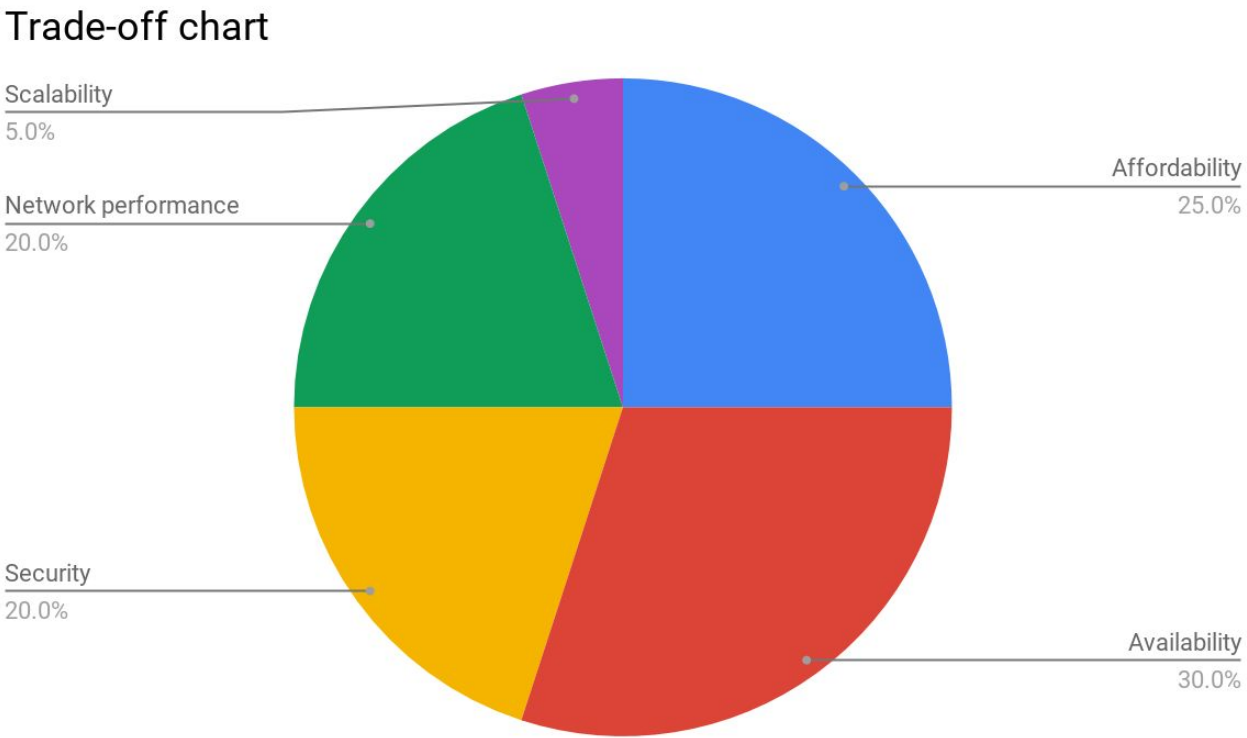

Doctor Cabins
Router
Patient Rooms
Paramount
Healthcare
Servers
Internal Applications
and Data
SaaS-based Medical Imaging
Software
Admin Staff
Finance Team
Operating
Theaters

Technical Goals

- Availability
- Affordability
- Network Performance
  - Throughput
  - Efficiency
  - Response time
- Security
- Minimising MTTR and Maximising MTBF
- Scalability



Technical Goals



Design Choices

- Hierarchical Network - 3 Layer Design
- UTP cables
- Commodity switches
- Additional servers
- Load Balancers
- Redundant routers
- Access control lists for security
- Firewall and IDS systems

Design Choices

After putting some thought into the physical routers and switches that will be used in our network, we have chosen the following:

- **Cisco 2811 Router**
  - Enhanced performance and high reliability
  - On-board encryption
  - Support for a variety of modules

- **Cisco 2960-24TT Switch**
  - 24 Fast Ethernet ports for maximised connectivity
  - 32 Gbps switching capacity

Costing

- **Cisco 2960 24TT Switch** (x8) | INR 7000 x 8 = INR 56,000
- **Cisco 2811 Catalyst Router** (x4) | INR 12,000 x 4 = INR 48,000
- **D-Link DES 1005C Switch** (x14) | INR 549 x 14 = ~ INR 7,700
- **TP-Link TL-R47TT Load Balancer** (x1) | INR 2,500 x 1 = INR 2,500
- **Internet connection** | ACT Entertainment Package 75Mbps | INR 14,000 per year
- **Miscellaneous** (Wi-fi, cables, installation) | INR 25,000

Trade-offs

- **Availability vs Affordability**
  To meet high expectations for availability, redundant components are often necessary, which raises the cost of network implementation.
- **Throughput vs Affordability**
  To have all applications running at full bandwidth would require separate cables from servers to each of the systems. This would increase costs.
- **Security vs Affordability**
  It is important to secure sensitive financial data and would require separate cables running from servers to finance officers. We try to maximize affordability.

Touchpoint 2

Assumptions and Approaches

1. Assuming single fail-safe ISP is available.
2. Replication of the servers is expensive, thus we are will not be duplicating the servers.
3. To avoid introducing single point of failure in the design we are assuming that the two servers are running identical applications.
4. Assuming 24/7 power supply. No power failures.
5. Since Network segmentation is expensive, we will not be implementing that for the time being.
6. Assuming SaaS software resides on local replicated servers.
7. We are not handling switch failure, as it requires a lot of processing power.

Access Control List

Stakeholders

1. Doctor
2. Nurse
3. Patient
4. Administration Staff
5. Finance Staff
6. Superuser

   Person with special privileges to maintain the system.

Access Control List

Network	Permitted (Incoming)	Denied (Incoming)
Doctor (10.10.1.0)	all	none
Admin (10.10.2.0)	Finance, Servers	Doctors, Operating Room
Finance (10.10.3.0)	none	all
Operating Room (10.10.4.0)	all	none
Servers (10.10.5.0)	all	none

Access Control List

Assets (Objects)

- **Patient Profile**
  Personal and demographic details of the patient.
- **Employee Profile**
  Personal, demographic, experience and employment data of the employee.
- **Salary Data**
  Salary details of the employee.
- **Patient Medical Data**
  Test results and medical information related to patient stored in database.
- **Internet Access**
  Access to internet through PESU Internet Captive Portal.
- **Medical Imaging Software**
  SaaS-based medical imaging software.
- **Access Control**
  Definition of privileges and permissions granted to stakeholders to access resources.
- **Daily Transaction Data**
  Finance related information of the hospital.
- **Network Health Information**
  Network related information of the hospital.

Access Control List

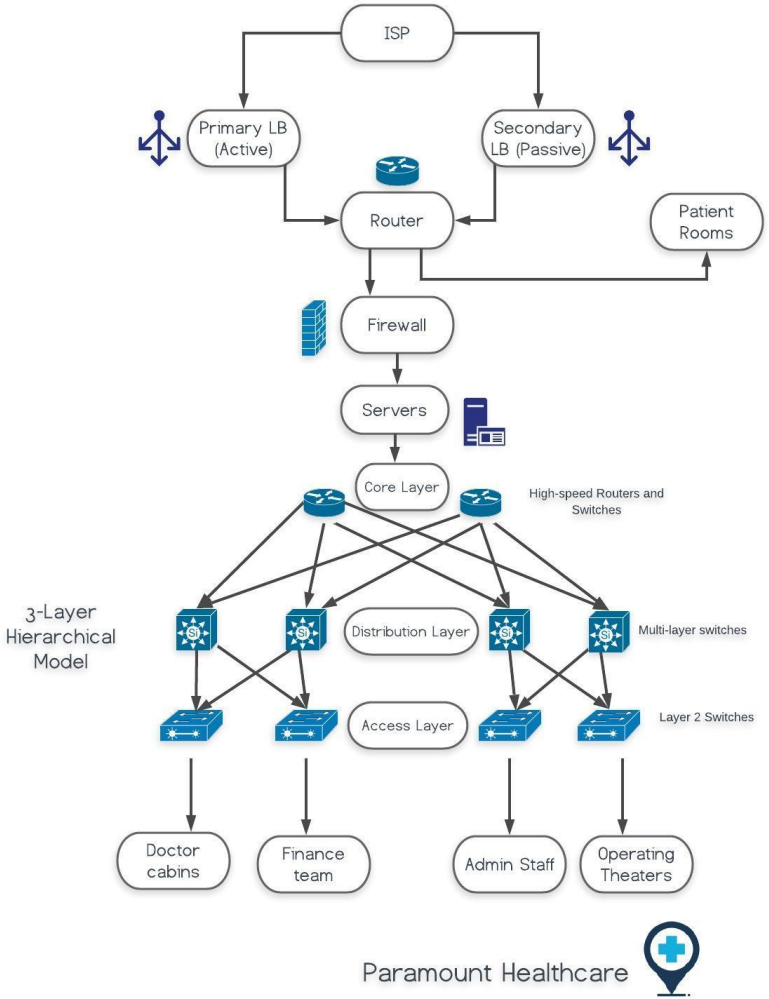
Operations

- **Read (View) - R**
  Ability to view data or content.
- **Write (Append) - W**
  Ability to add a record (or add a table to the database).
- **Modify - M**
  Ability to modify records (or database definition).
- **Delete - D**
  Ability to delete a record (or a table or a resource, as applicable).
- **Execute - E**
  Ability to execute or use a resource. (Applicable to certain types of resources).

Access Control Matrix

Roles \ Assets	Patient Profile	Employee Profile	Salary Data	Patient Medical Data	Internet Access	Medical Imaging Software	Daily Transaction Data	Network Health Information	Access Control
Doctor	R	R M	R	R W M D	R	R	-	-	-
Nurse	R	R M	R	R	R M	R	-	-	-
Patient	R W M D	R	–	R	R M	-	-	-	-
Administration Staff	R	R W M D	R	R	R W M D E	-	-	R	R W M D E
Finance Staff	R	R M	R W M D	-		-	R W M	-	-
Superuser	R	R W M D	R W M D	R W M D	R W M D E	R	R W M	R	R W M D E

Proposed Logical Design



(Note: Revised later)

Network IP Address Designation

ELEMENT	GROUP	IP
PC1	DOCTOR	10.10.1.1
PR1		10.10.1.2
PC2	/24	10.10.1.3
PR2	MASK: 255.255.255.0	10.10.1.4
PC3	GATEWAY: 10.10.1.254	10.10.1.5
PR3		10.10.1.6
PC4		10.10.1.7
PR4		10.10.1.8
PC5		10.10.1.9
PR5		10.10.1.10
PC1	ADMIN	10.10.2.1
PR1		10.10.2.2
PC2	/24	10.10.2.3
PR2	MASK: 255.255.255.0	10.10.2.4
PC3	GATEWAY: 10.10.2.254	10.10.2.5
PR3		10.10.2.6
PC1	FINANCE	10.10.3.1
PR1	/24	10.10.3.2
PC2	MASK: 255.255.255.0	10.10.3.3
PR2	GATEWAY: 10.10.3.254	10.10.3.4
PC1	OPERATING ROOM	10.10.4.1
PC2	/24	10.10.4.2
PC3	MASK: 255.255.255.0	10.10.4.3
PC4	GATEWAY: 10.10.4.254	10.10.4.4
SERVER1	SERVER /24	10.10.5.1
SERVER2	MASK: 255.255.255.0	10.10.5.2
	GATEWAY: 10.10.5.254	

ROUTER 1						
PORTS	FA 0/0	FA 1/0	FA 2/0	FA 3/0	FA 4/0	FA 5/0
IP	10.10.6.2	10.10.1.253	10.10.2.253	10.10.3.253	10.10.4.253	10.10.5.253
NETWORK	N6	N1: DOCTOR	N2: ADMIN	N3: FINANCE	N4: OR	N5: SERVER
NETOWRK IP	10.10.6.0	10.10.1.0	10.10.2.0	10.10.3.0	10.10.4.0	10.10.5.0
PRI: 105	GR 6	GR 1	GR 2	GR 3	GR 4	GR 5

ROUTER 2						
PORTS	FA 0/0	FA 1/0	FA 2/0	FA 3/0	FA 4/0	FA 5/0
IP	10.10.6.3	10.10.1.252	10.10.2.252	10.10.3.252	10.10.4.252	10.10.5.252
NETWORK	N6	N1: DOCTOR	N2: ADMIN	N3: FINANCE	N4: OR	N5: SERVER
NETOWRK IP	10.10.6.0	10.10.1.0	10.10.2.0	10.10.3.0	10.10.4.0	10.10.5.0
PRI: 100	GR 6	GR 1	GR 2	GR 3	GR 4	GR 5

ALL GATEWAYS END WITH 254

FIREWALL		
PORTS	FA 0/0	FA 1/0
IP	10.10.6.1	10.10.7.1
NETWORK	N6	N7
NETOWRK IP	10.10.6.0	10.10.7.0

ISP	
PORTS	FA 1/0
IP	10.10.8.1
NETWORK	N8
NETOWRK IP	10.10.8.1
GATEWAY	10.10.8.254

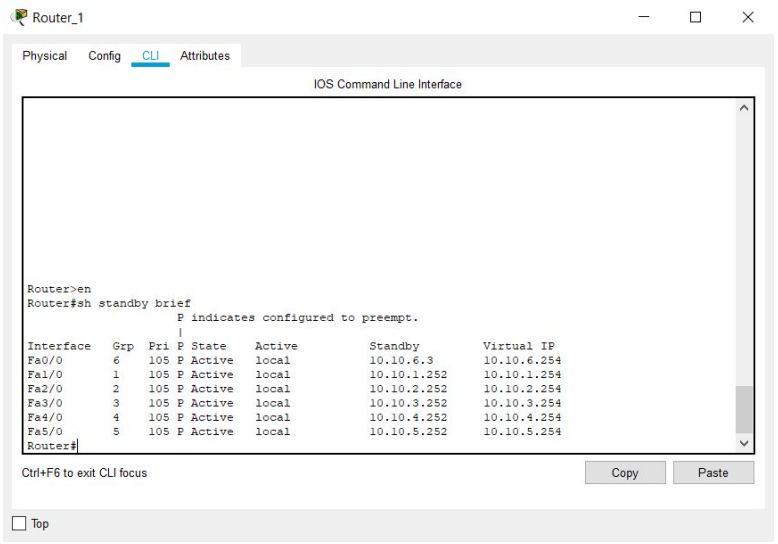
WIFI	
PORTS	INTERNET
IP	10.10.7.253
NETWORK	N8
NETOWRK IP	10.10.7.0
GATEWAY	10.10.7.254

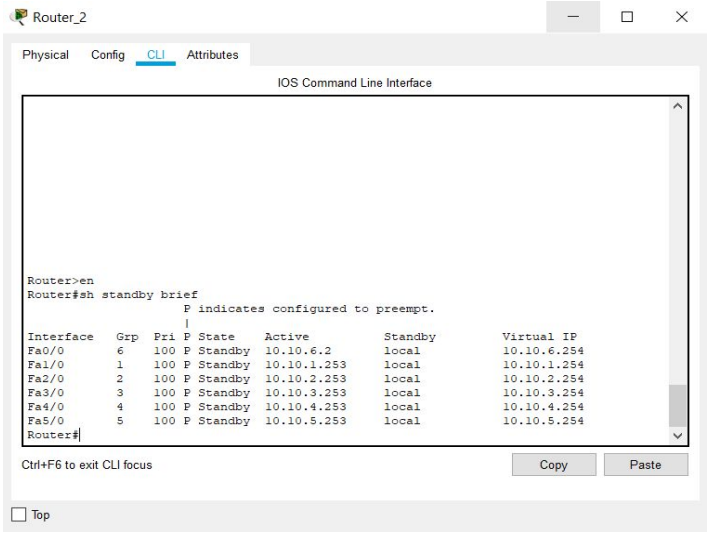
ISP ROUTER 1		
PORTS	FA 0/0	FA 0/1
IP	10.10.8.2	10.10.7.2
NETWORK	N8	N7
NETOWRK IP	10.10.8.0	10.10.7.0

ISP ROUTER 2		
PORTS	FA 0/0	FA 0/1
IP	10.10.8.3	10.10.7.3
NETWORK	N8	N7
NETOWRK IP	10.10.8.0	10.10.7.0

HSRP

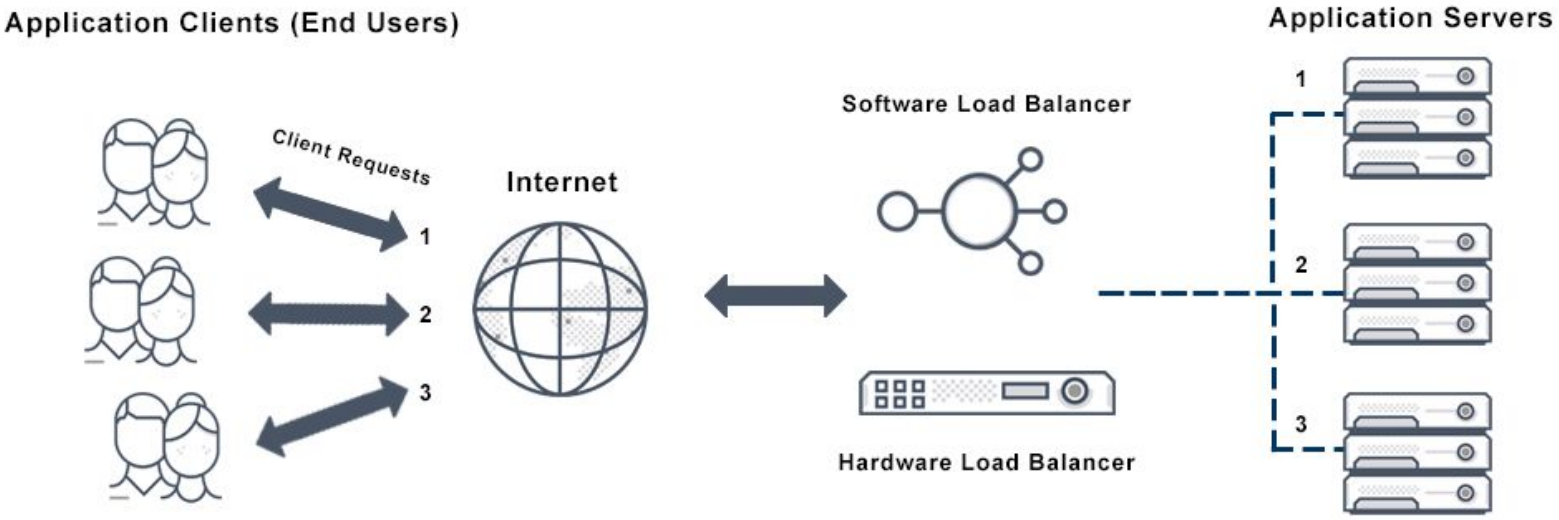
- Enabled HSRP in routers to provide high availability to client.
- Multiple routers behave as a single virtual router.





LOAD BALANCING

Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.



Thank you

Dweepa Prasad 01FB16ECS138

Ishita Bhandari 01FB16ECS143

Shashank Prabhakar 01FB16ECS356

Shrey Tiwari 01FB16ECS368