IK2215 Advanced Internetworking
ISP Project
Group 3

Group Members:

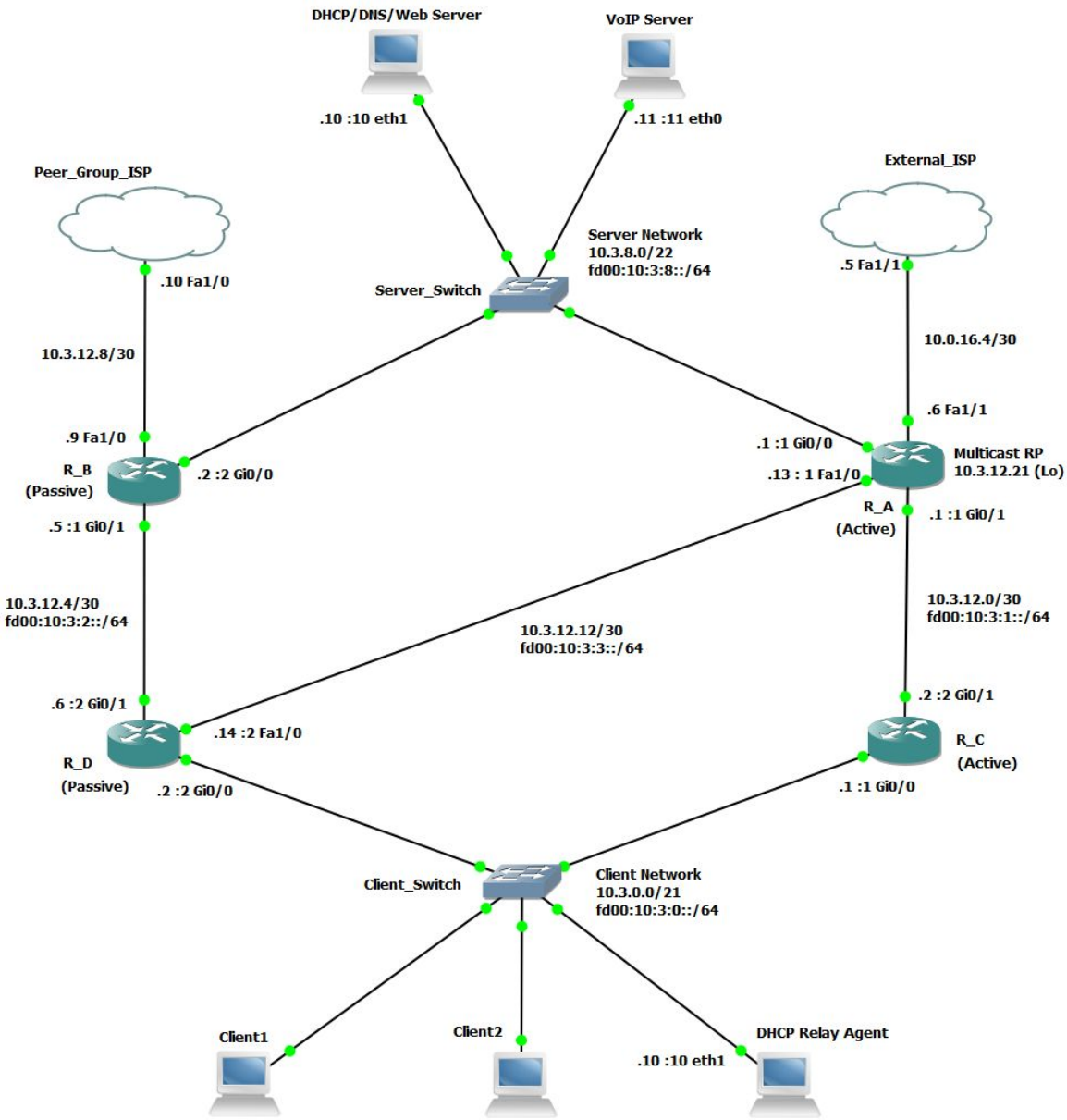
Borek, Martin	borek@kth.se
Golinski, Anne	golinski@kth.se
Gunnari, Joakim	jgunnari@kth.se
Liu, Zhehuan	zhehuan@kth.se
Omer Mahgoub Saied, Khalid	koms@kth.se
Tatsis, Nikolaos	ntatsis@kth.se
Yang, Haiyan	haiyany@kth.se

1. Detailed network topology

1.1 Required equipment

4 x Cisco 7301 routers.
2 x HP2524 switches.
4 x lab VMs.
8 x UTP straight cables, 2 x UTP cross cables.
External server for the VoIP running on a personal laptop, and two additional personal laptops.

1.2 Network map



We have assumed that the majority of the traffic will be in-house, and hence the Gigabit ethernet link is used for the internal ISP connection. Fast ethernet links are used to connect to the external ISP and the peer group ISP and an additional fast ethernet link is also added diagonally in our square shaped network setup to provide redundancy in the internal network. The patch panel will be connected as follow:

From port:	To port:	Comment:
5	17	router A Gi0/0 to the server switch
6	18	router B Gi0/0 to the server switch
7	21	router C Gi0/0 to the client switch
8	22	router D Gi0/0 to the client switch
9	11	router A Gi0/1 to the router C Gi0/1
10	12	router B Gi0/1 to the router D Gi0/1
13	16	router A Fa1/0 to the router D Fa1/0
14	link to the peer AS router	router B Fa1/0 to router X Fa1/0

1.3 IP address allocation

IPv4: Our major subnet is 10.3.0.0/20. We allocate 2046 host addresses on the 10.3.0.0/21 client subnet and 1022 host addresses on the 10.3.8.0/22 server subnet. Then we use three additional /30 subnets, 10.3.12.12/30, 10.3.12.4/30 and 10.3.12.0/30 for connecting the routers within our network, and 10.3.12.8/30 for connecting router B with the peer ISP. The reason why we chose to divide the addresses this way is to make sure that we have allocated enough addresses for our clients and to make sure that possible server hosting services are available to the clients.cccvx

IPv6: Our major subnet is fd00:10:3::/48. We have chosen two /64 subnets for the server side (fd00:10:3:8::/64) and client side (fd00:10:3:0::/64). Another three /64 subnets were used for the router connections (fd00:10:3:1::/64, fd00:10:3:2::/64 and fd00:10:3:3::/64).

Router interface IP address assignment:

Device	**Interface**	**IPv4 Address**	**IPv6 Address**	**Hostname**
R_A	Gi0/1	10.3.12.1/30	fd00:10:3:1::1/64	gi01_ra.isp3.lab
R_A	Gi0/0	10.3.8.1/22 + (VIP 10.3.8.3)	fd00:10:3:8::1/64 + (VIP fe80::1)	gi00_ra.isp3.lab
R_A	Fa1/1	10.0.16.6/30		fa11_ra.isp3.lab
R_A	Fa1/0	10.3.12.13/30	fd00:10:3:3::1/64	fa01_ra.isp3.lab
R_A	Loopback	10.3.12.21/32	fd00:10:3:12::21/128	loopback_ra.isp3.lab
R_B	Gi0/1	10.3.12.5/30	fd00:10:3:2::1/64	gi01_rb.isp3.lab
R_B	Gi0/0	10.3.8.2/22 + (VIP 10.3.8.3)	fd00:10:3:8::2/64 + (VIP fe80::1)	gi00_rb.isp3.lab
R_B	Fa1/0	10.3.12.9/30		fa01_rb.isp3.lab
R_B	Loopback	10.3.12.22/32	fd00:10:3:12::22/128	loopback_rb.isp3.lab
R_C	Gi0/1	10.3.12.2/30	fd00:10:3:1::2/64	gi01_rc.isp3.lab

R_C	Gi0/0	10.3.0.1/21 +(VIP 10.3.0.3)	fd00:10:3:0::1/64 + (VIP fe80::1)	gi00_rc.isp3.lab
R_C	Loopback	10.3.12.23/32	fd00:10:3:12::23/128	loopback_rc.isp3.lab
R_D	Gi0/1	10.3.12.6/30	fd00:10:3:2::2/64	gi01_rd.isp3.lab
R_D	Gi0/0	10.3.0.2/21 +(VIP 10.3.0.3)	fd00:10:3:0::2/64 + (VIP fe80::1)	gi00_rd.isp3.lab
R_D	Fa1/0	10.3.12.14/30	fd00:10:3:3::2/64	fa01_rd.isp3.lab
R_D	Loopback	10.3.12.24/32	fd00:10:3:12::24/128	loopback_rd.isp3.lab

Servers and clients IP address assignment:

Device	IPv4 Address	IPv6 Address	Hostname
DNS / DHCP / Web Server	10.3.8.10	fd00:10:3:8::10	ns.isp3.lab
DHCP Relay Agent	10.3.0.10	fd00:10:3:0::10	dhcp-relay.isp3.lab
VOIP Server	10.3.8.11	fd00:10:3:8::11	voip.isp3.lab
Client1	10.3.0.11	fd00:10:3::11	client-1.isp3.lab
Client2	10.3.0.12	fd00:10:3::12	client-2.isp3.lab

2. Mandatory tasks

2.1 Routing functionality

2.1.1 Dynamic IP routing

Open Shortest Path First (OSPF) is chosen as the routing protocol for the network. That is because the fast convergence and scalability features of OSPF makes it more suitable for ISPs than distance vector protocols. Since the network is small, all the routers are configured in OSPF area 0. To prefer Gigabit ethernet links over fast ethernet links the reference bandwidth is set to 1000 Mbps on all routers. This means that the OSPF cost will be 1 for Gigabit ethernet links and 10 for fast ethernet links. OSPF will be configured to distribute the loopback address of the routers in order for them to be used as the source address for the iBGP connection.
For internal routing the primary path used is through routers R_A and R_C. The link between routers R_B and R_D is a backup link used if the link between routers R_A and R_C would fail (see 2.1.2 Fault-tolerant IP routing). There is also a second backup link between routers R_A and R_D that is only used if the two links described above would be down at the same time.
EBGP will run between router R_A and the external primary ISP and between router R_B and the peer ISP. iBGP will run between routers R_A and R_B. The BGP connection will provide redundant connection to the other ISPs as well as a transit ISP service to the peer ISP in case of failures in their primary ISP connection. BGP will be configured with some policies to achieve this. First router R_B will have an outgoing policy that will lengthen the AS path to discourage the peer ISP from choosing our network. Since we can not guarantee that the peer ISP will implement a similar policy, we use an additional policy in router R_B

that will prefer the BGP routes coming from router R_A over the ones from the peer ISP. Both router R_A and router R_B will distribute the BGP routes into OSPF, but with different metrics for each router. BGP will advertise the aggregate OSPF to the external peers. This setup will provide high degree of redundancy.

2.1.2 Fault-tolerant IP routing

Hot Standby Router Protocol (HSRP) is chosen to apply fault-tolerant IP routing since it is a Cisco proprietary protocol and provides automatic backup on routers when configured over Ethernet, Fiber Distributed Data Interface (FDDI) and Token Ring local-area networks (LANs).
HSRP is enabled on both the client and server side of the network, with routers R_A and R_C configured as active routers, and routers R_B and R_D configured as standby routers. Object tracking is configured so that if the link between router R_C and router R_A fails, router R_D and router R_B will change status from standby to active.
R_A and R_C are chosen as master routers, this means that under normal conditions, the traffic designated to outside our internal ISP network will follow the most efficient path.

2.1.3 PIM-SM IP Multicast routing

PIM-SM is suitable for an ISP since it is scales well, it builds unidirectional shared trees rooted at a Rendezvous Point (RP) per multicast group, instead of implicitly building shortest path trees using multicast flooding. PIM-SM can also optionally create shortest-path trees per source, meaning that multicast traffic can be sent directly from the source to the multicast receivers without going through the RP, thus reducing network latency and eventual congestion at the RP.
The RP which is utilized when sending multicast traffic, will be assigned to router R_A. We want the RP to be centralized in the network, close to our sending sources in the server network. To protect the RP, it will be configured on router R_A's loopback interface with address 10.3.12.21. This is because a software interface is less likely to go down than a physical link.
To ensure that we have multicast routing only within our network, PIM-SM will not be run on interfaces connected to other AS's.

2.2 Internet application services

2.2.1 DNS

We are planning to use the BIND application for our domain name servers as it is the standard for Unix-like operating systems and the most widely used name server software. Moreover, it is an open source software developed by the Internet Systems Consortium. We will be running the BIND application on a Ubuntu linux distribution. The DNS server will be used for assigning names to hosts, servers and routers within our network.
The DNS will be configured to forward all the DNS lookup to the primary ISP DNS for domains outside our ISP domain (isp3.lab).

2.2.2 DHCP

DHCP will be handled by running the DHCP daemon (dhcpd) on one centralized DHCP server and on one DHCP relay server. The centralized DHCP server is located in a server network and assigns IPv4 and IPv6 addresses to servers and clients. The DHCP relay server is located in a client network and is used for forwarding packets between the centralized DHCP server and clients. Both these servers will be running on the Ubuntu platform. We have chosen the dhcpd because it is a standard for Linux operating systems and it is developed and maintained by the Internet Systems Consortium.

2.2.3 Web server

We are planning to use an Apache server running on one of the Linux virtual machines. Apache is one of the most popular web server implementations, highly optimized and tested for all circumstances. The web server will offer access to a web page containing our project plan, both to clients inside the network and any other host outside of it.

3. Selective tasks

3.1 IPv6

To implement Ipv6 in our network we are using IPv4/IPv6 dual stack. OSPFv3 is chosen as the routing protocol with similar motivation as for OSPF version 2. Fast convergence and scalability features makes it more suitable for ISPs that distance vector protocols. By choosing OSPFv3 for IPv6 we are also consistent in our choice of network IGPs. Using dual stack means that both IPv4 and IPv6 packets can be routed within our network the same way. See section 1.3 IP address allocation for details on how the IPv6 address block have been divided within the network.

3.2 VoIP

VoIP is an essential service provided by many ISPs, who usually also serve as telephony providers.
We will be using the FreePBX Linux Distro 6.12.65, running FreePBX 12 and Asterisk 11, and the client will connect through the SIP protocol. We have chosen FreePBX as our VoIP server implementation for the following reasons: Firstly, we wanted an open source implementation, since that ensures security through the participation of multiple developers who can identify and fix security holes. Secondly, we wanted a server which would offer an easily accessible interface to modify the server parameters, something that FreePBX is designed to do. It's also a front-end to Asterisk, which offers a large amount of features, both in supported protocols and in implemented features. Lastly. a large active developer base provides future proofing, something important to us as we are emulating an ISP.
For our demonstration, we will showcase a voice call between two clients, first by using IPv4 and then IPv6. A call to another group providing VoIP as its selective task, is also possible.