RCOMP - Redes de Computadores

(Computer Networks)

2020/2021

Project description - sprint 3

In this sprint, each team member will keep working on the same network simulation from the previous sprint (regarding the same building). From the already established layer three configurations, now OSPF based dynamic routing will be used to replace static routing used previously.

Beyond OSPF based dynamic routing, other configurations encompassed in this sprint are:

- DHCPv4 service
- VoIP service
- Adding a second server to each DMZ network to run the HTTP service.
- Configuring DNS servers to establish a DNS domains tree.
- Enforcing NAT (Network Address Translation).
- Establishing traffic access policies on routers (static firewall).

1. OSPF dynamic routing

Static routing will no longer be used, thus on every router, the existing static routing tables should be erased, the only exception is the default route established in the **building 1** router.

The overall infrastructure will become now an OSFP domain (Autonomous System), it will be split into OSPF areas, one for each building, and the backbone area (area id 0).

The backbone area (area id 0) encompasses only one IPv4 network, the backbone VLAN. For each building an area id must be assigned, each of these areas will encompass all IPv4 networks within the corresponding building.

OSPF area ids to be used in each building should be settled on the planning meeting, even though each building is not required to be aware of the area ids used in other buildings, they can´t be the same.

The team member in charge of building 1 must insert into the OSPF routing protocol the default route, pointing to the ISP router (default-information originate).

2. HTTP servers

In addition to the already existing server, in each building, a new server must be added to the local DMZ network, as the former, it will have a manually set IPv4 address. On this server, the HTTP service must be enabled, and a simple HTML page should be created, at least identifying it as belonging to the building it does.

3. DHCPv4 service

The router in each building must provide the DHCPv4 service to all local networks (within the building), except for DMZ networks and the backbone where IPv4 node addresses are static and manually set (routers and servers).

For the VoIP VLAN, the DHCP server configuration has to include **option 150**, it represent the IP address of the TFTP (Trivial File Transfer Protocol) server to be used by Cisco IP phones model 7960 to download their configuration file.

4. VoIP service

The router in each building provides the VoIP service (Cisco Telephony) to the local VoIP network (within the building), this encompasses calls forwarding to other buildings (other buildings' routers with the VoIP service).

In the simulation, for VoIP local testing, in each building there should be at least two connected IP phones (please, use the 7960 model available in Packet Tracer).

Ports of switches connecting to Cisco IP phones 7960, must have the **voice VLAN** enabled (switchport voice vlan VLANID) and the **access VLAN** disabled (no switchport access vlan).

Regarding VoIP call forwarding, when an incoming call is for a phone prefix assigned to another building, then the call must be forward to the telephony services running in that building router.

5. DNS

Independent DNS domains are going to be established on each building.

The team member in charge of building 1 will create a DNS domain name matching the team's repository name (**rcomp-20-21-cc-gn**). This is going to be the highest level domain, so it's going to be used as if it was the DNS root domain.

Team members in charge of other buildings will create local DNS domains named as:

building-X.rcomp-20-21-cc-gn

With X replaced by the digit that identifies the building.

So these are subdomains of the **rcomp-20-21-cc-gn** domain.

In each building, there must be a DNS name server to support the local DNS domain, the server that was added to each DMZ, on the previous sprint, should be used.

All DNS servers should have the unqualified DNA name **ns**, so for building 1 it will be **ns.rcomp-20-21-cc-gn**, and for instance for building 3 it will be **ns.building-3.rcomp-20-21-cc-gn**.

Additional required information to establish the DNS tree (and make DNS name servers work together):

- The DNS server for domain **rcomp-20-21-cc-gn** (building 1) must know the IPv4 addresses of the name servers of its subdomains (each one in each of the other buildings).
- The DNS servers of other domains (other buildings) must know the IPv4 address of the name server of the **rcomp-29-21-cc-gn** domain.

The last requirement comes from the fact that the rcomp-20-21-cc-gn domain is going to be used as DNS root domain. Remember every DNS server must know the root name servers.

Surely IPv4 addresses for these servers have already been established in the previous sprint, but they should be now clearly registered on this sprint planning. The team member in charge of building 1 will need them all, other team members will need only the IPv4 address of the DNS name server in building 1.

Within DNS databases, all names must be FQDN (fully qualified domain names), so for each team every name defined in DNS databases on every name server must end up with **rcomp-20-21-cc-gn**.

The team could decide to add a final dot (standing for the root: **rcomp-20-21-cc-gn.**), though this is not coherent because would assume **rcomp-20-21-cc-gn** was a top level domain, and that's not true. If the team decides to add a dot, then it should be added on every DNS name on all DNS databases, otherwise domains won't be on the same branch.

5.1. NS (Name Server) records and glue records

The way DNS works requires every domain to know the name servers of each of its subdomain, and also to know the name servers of the root domain. Knowing a name server that is out of the scope of the local domain requires is in fact two DNS records:

- **The NS record itself**: the record's name is the domain's name and the record's data is the DNS name of the name server of that domain.
- **The A record for the NS record**: the record's name is the DNS name of the name server and the record's data is the IPv4 address the name server.

The last one is usually called a glue record, it's required because the NS record doesn't provide an IP address, yet that is required to contact the name server. In this case DNS name servers are using IPv4 only, if they were using IPv6, then there should be also an AAAA glue record as well.

5.2. Other DNS records

All HTTP servers are to be named **server1** (A record), it's perfectly ok they all having the same name because they belong to different DNS domains.

Within each DNS domain there should be a **www** alias (CNAME) mapped to the same domain's **server1** A record, and another alias, named **web** also mapped to the domain's **server1** A record.

One additional alias (CNAME), with name **dns**, and mapped to the domain's **ns** A record, should also exist.

5.3. DNS clients' configuration (end-nodes)

All end-nodes within a building should be using the local DNS name server, and, if supported, have the default DNS domain name set to the local DNS domain name.

For end-nodes with automatic DHCP configuration, that information should be inserted into the local DHCP pools (**dns-server** and **domain-name** commands).

For end-nodes with static manual configuration, i.e. servers, that information must be added manually.

6. NAT (Network Address Translation)

NAT can have several uses, and it's often enforced to hide private addresses (dynamic NAT). Static NAT, on the other hand, can be used to redirect traffic, and that's what will be applied in this sprint.

Each router's administrator (team member managing a building) will enforce the required configurations so that:

HTTP and HTTPS requests received in the router's backbone interface are redirected to the HTTP server in the local DMZ. Both HTTP and HTTPS use TCP connections, assume the default service ports numbers are used, 80 and 443.

DNS requests received in the router's backbone interface are redirected to the DNS server in the local DMZ. The DNS service may use either UDP or TCP, but in either case the default service port number is 53. Both cases should be covered.

7. Static Firewall (ACLs)

In CISCO IOS, a static firewall establishes rules (Access Control Lists) regarding which individual packets are allowed to be received or sent through a network interface and which are not. It's called static or stateless because it always behaves the same way regardless of the transaction context in which the packet is analysed.

In must be emphasised that the enforcement of ACLs should be the last task in this sprint, only once the previously described features are in place and well tested, then this subtask should be embraced.

This is recommended approach because previously described features must still work once the ACLs are enforced. Thus, under troubleshooting point of view, by undertaking this method, the administrator knows any arising problem with previously described features is due to issues in firewall rules, and not the feature implementation itself.

Traffic access policies (which packets are allowed or not) are going to be implemented in routers, by the administrator in charge of each router. They will be particularly restrictive on traffic exchanged with the local DMZ, and traffic that is intended to the router itself.

In higher precedence first order, traffic access policies to be enforced are:

1st - Block all spoofing, as far as possible. Internal spoofing from local networks, the DMZ may be excluded. External spoofing in traffic incoming from the backbone network.

2nd - All ICMP echo requests and echo replies are always allowed.

3rd - All traffic to the DMZ is to be blocked, except for the DNS service and HTTP/HTTPS services to the corresponding servers. All traffic incoming from the DMZ is allowed.

4th - All traffic directed to the router itself (with a destination IPv4 node address belonging to the router) is to be blocked, except for the traffic required for the current features to work.

5th - Remaining traffic passing through the router should be allowed.

Regarding the 4th access policy exceptions, they will encompass several services that must be allowed for networks where they are required, some not to be forgotten are:

- The DHCPv4 service. Notice the first DHCPv4 request (DHCP discover) is sent from IPv4 source address 0.0.0.0 (unknown address) to the IPv4 destination address 255.255.255.255 (local broadcast).
- The TFTP service (for IP phones).
- The ITS service (for IP phones and for other IST servers).
- OSPF traffic.
- Traffic encompassed by the recently enforced NAT static rules.

8. Teamwork organization

Unlike what has been happening in previous sprints, now each team member should use as starting point the overall simulation resulting from sprint 2 (**`campus.pkt`**), nevertheless, each team member will be in charge of the same building as before.

Beyond the member's assigned building's router, each team member will also take the task of changing from static routing to OSPF based dynamic routing in every existing router, but no other changes are to be applied on those routers.

During the sprint planning meeting, the team must establish:

- The OSPF area ids to be used on each building (area id 0 is already assigned to the backbone network).
- VoIP phone numbers and prefix digits schema. Each building should have a different prefix digit, to configure calls forwarding to other buildings
- The DNS domain names to be used (the highest level domain should be the team's repository name: **rcomp-20-21-cc-gn**).
- The IPv4 node address of the DNS name server of each DNS domain. The name of the domain's DNS name server has already been established to be **ns** within that domain.

All these data must be registered in the **planning.md** document for sprint 3.

The team member is charge of **building 2** has the additional final subtask of integrating all members work for this sprint into a single overall simulation (**campus.pkt**). It's a copy and paste operation between Packet Tracer instances.

The best option for cutting points is the connection of each building to the backbone network, each building's main switch should be kept and the backbone connections between those switches rebuilt. Bear in mind connections between all switches must be in trunk-mode.

9. Sprint 3 backlog

Task	Task description
T.3.1	Update the **campus.pkt** layer three Packet Tracer simulation from the previous sprint, to include the described features in this sprint for building 1.
T.3.2	Update the **campus.pkt** layer three Packet Tracer simulation from the previous sprint, to include the described features in this sprint for building 2. Final integration of each member's Packet Tracer simulation into a single simulation.
T.3.3	Update the **campus.pkt** layer three Packet Tracer simulation from the previous sprint, to include the described features in this sprint for building 3.
T.3.4	Update the **campus.pkt** layer three Packet Tracer simulation from the previous sprint, to include the described features in this sprint for building 4.
T.3.5	Update the **campus.pkt** layer three Packet Tracer simulation from the previous sprint, to include the described features in this sprint for building 5.

Task T.3.5 is to be ignored by teams with 4 members only.

10. Sprint 3 outputs/products

For each task on this sprint, the main output is the Packet Tracer simulation file for the corresponding building, it should be named **buildingN.pkt**, with N replaced by the digit identifying the building. Each team member is to commit that file into the personal sprint folder.

A document (any standard format) detailing DNS databases records on the building's DNS name server, it may be a screenshot of the server's DNS database.

Each team member must also commit to the personal sprint folder a text file with a configuration dump for every switch and for every router within the encompassed building. These configuration text files can be easily exported in Packet Tracer: within the device's window click the **export** button on the **Running Config**, or the **Startup Config** (if the **Running Config** has been saved).

The default name for the text file may be kept, as it represents the device's display name. During the sprint members are to commit changes to these files as they change their devices' configurations. This also acts as a safeguard, if somehow the configuration of devices in Packet Tracer is lost, it may be restored from these files.

For task **T.3.2** there's one additional output to be committed into the personal sprint folder, it's the overall simulation integrating all members work, that file should be named **campus.pkt**. Regarding configuration files and other configuration details, for task T.3.2, they only encompass devices from building 2.