Network Laboratory

Ruizhi Liao, Alex Bikfalvi, Jaume Barcelo, Albert Rabassa

Spring 2014

Last updated: May 13, 2014

Contents

Acknowledgements

The assignments presented in this book are the ones that have been prepared over the years in the Network Laboratory course by different instructors, including Anna Escudero, Anna Sfairopoulou and Eduard Bonada.

Chapter 1

About the Course

1.1 Course Data

Code: 21728
Course name: "Laboratori de Xarxes i Serveis"
Teachers: Ruizhi Liao, Alex Bikfalvi and Jaume Barcelo
Credits: 4
Year: 2nd year
Trimester: Spring

1.2 Introduction

The goal of this course is to acquire hands-on experience with networking equipment such as *access points*, *switches*, *routers* and *firewalls*. The students should be familiar with the high-level functionality of each of these devices. The actual configuration of the equipment and the construction of prototype networks will provide further insights into the operation of these network devices. After the course, the student will be ready to plan and configure a small network.

1.3 Syllabus

- Lectures
    1. Introduction, Traffic analysis and IEEE 802.11 WLANs
    2. Virtual Local Area Networks and Spanning Tree Protocol
    3. Routers
    4. Firewalls
    5. Test and Final Project
- Lab Assignments

1. Traffic analysis
2. IEEE 802.11 Wireless Local Area Networks (WLANs)
3. Virtual local area networks (VLANs)
4. Spanning Tree Protocol (STP)
5. Routing
6. Firewalls

1.4 Bibliography

- J. Kurose, K. Ross, "Computer Networking"
- "Cisco Networking Academy Program: CCNA 1 and 2 companion guide"
- "Cisco Networking Academy Program: CCNA 3 and 4 companion guide"

1.5 Evaluation Criteria

The final grade is distributed as follows.

Evaluation Method	Weight
Lab assignments	70 %
Continuous assessment quiz	10 %
Final exam	20 %

The students need to obtain a passing mark (half of the available points) in all the different evaluation aspects.

1.6 Group Work

The assignments are done in groups of three students. A single report is delivered for each group. It is important that all the members of the group participate in the experiments and the preparation of the report. The teachers may ask individual questions to the students in the labs, and both the quiz and the final exam are performed individually.

1.7 Lab Report

For each lab assignment, it is necessary to prepare a lab report answering all the questions. The students are also expected to include additional information, explanation and comments besides those explicitly asked in the assignment.

1.8 The Lab

The networking lab has PCs, wireless access points, switches, routers, firewalls and a patch panel to make the connections. The user for the computers is `administrador`. The password for the computers is `pompeulab`. The root password for Linux is `pompeulab`.

1.9 Survival guide

1.9.1 Questions and Doubts

We like to receive questions and comments. Normally, the best moment to express a doubt is during the class, as it is likely that many people in the class share the same doubt. If you feel that you have a question that needs to be discussed privately, we can discuss it right after the class.

1.9.2 Continuous Feedback

At the end of lectures, we will ask you to provide some feedback on the course. In particular, we always want to know:

- What is the most interesting thing we have seen in class.
- What is the most confusing thing in the class.
- Any other comment you may want to add.

1.9.3 How to Make Your Teachers Happy

Avoid speaking while we are talking.

Part

I

Classroom Sessions

Chapter 2

Traffic Analysis, LAN, WLAN

2.1 Traffic Analysis

2.1.1 Layered Networks

Data networks are organized in layers. These layers communicate with each other using interfaces. Each layer offers some services to the layer on top of it. Also, each layer in one end of the communication connects to the same layer at the other end of the communication.

In theory, the layers are relatively independent from each other. A layer can see other layers as *black boxes* without having to care about implementation details. This approach is a common practice in engineering as it allows each team of engineers to focus in a particular problem which is just a piece of a puzzle to solve a bigger problem.

Each layer accomplishes some particular tasks. For example, the link layer is responsible for one hop connectivity. The network layer is assigned the task of taking routing decisions to move packets from one network to the other.

The Open Systems Interconnection model (OSI) partitions a communication system in seven layers: physical, data link, network, transport, session, presentation and application. The TCP/IP model (Transmission Control Protocol/Internet Protocol) is more specific to the Internet and differentiates four layers: link, network, transport, and application.

The link layer is in charge of one-hop communication. The network layer is responsible for connecting multiple networks and therefore should be capable of routing data through multiple hops. The transport network takes care of end-to-end communication between two hosts, and can multiplex different instances of communications in each host. The application layer uses the end-to-end communication to offer some kind of service to the network user.

In practice, data transmitted over data networks is divided in chunks of information. It can be convenient to give different names to the different chunks of information used by the different layers: frames (LINK), IP packet (NET), UDP datagram or TCP segment (TRA), and message (APP).

The application messages are encapsulated in TCP segments or UDP datagrams which, in turn, are encapsulated into IP packets that are finally encapsulated into link layer frames. Regular users do not need to worry about all these data chunks and encapsulation and de-encapsulation

processes. However, for network engineers designing systems or debugging networks it is very useful to peek into the data chunks of all communications layer to find the errors.

2.1.2 Coexistence of Protocols

In the network coexist a multitude of protocols. Obviously, we need protocols of different layers to achieve communication. But even within a particular layer, we find coexisting protocols.

For example, we will make use of FTP (file transfer) and HTTP (hypertext) in our labs.

A particular case is that of the network (or Internet) layer. This is the protocol that provides end-to-end connectivity and for many years the IPv4 has totally dominated network. The associated Internet Control Message Protocol v4 (ICMPv4) has friendly coexisted with IPv4.

Today there is a strong incentive to have another protocol, in particular IPv6, at the network layer because IPv4 address space is exhausted. However, for IPv6 to be useful it is necessary that all the routers in the communication path support. If IPv6 is not supported end-to-end, it is necessary to resort to tunneling or translation techniques that increase the complexity of the communication. For this reason, many network administrators are waiting for others to enable IPv6 first. As a result, the adoption of IPv6 has been too slow.

2.1.3 Traffic Analysis

There are some useful tools to analyze the traffic in our networks. Two of them are tcpdump (command line) and wireshark (graphic interface). This tools capture the packets of one or more interfaces and analyze the protocols at all layers.

It is possible apply capture filters in order to capture only those packets that are of interest. In wireshark, it is also possible to apply display filters. In the case of display filters only some of the stored packets are shown, but the rest of the data is still available and will be visible if the display filter is changed. In the case of capture filters, packets that do not fit the filter criteria are discarded and cannot be recovered for analysis at a later time.

2.1.4 iptables

Iptables is a linux tool that can be used to manage IP packets in the device. It can be used to drop packets, modify them and/or redirect them. The packets can be intercepted at different places: PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING In each of this places, the system administrator can configure a set of rules and actions for the packets that match the rules.

Typical uses of iptables include the implementation of firewalls and network address translation (NAT).

2.1.5 Proxy

A proxy is a relay working at the application layer. The proxy caches content and can speed up web browsing and upstream bandwidth when accessing static content. A university or other institution can use a proxy with a port configuration different than 80. This aspect needs to be taken into consideration when analyzing web traffic.

2.1.6 Connection Oriented Protocols

Even though the communication occurs using data packets, some protocols are connection oriented. These protocols have a previous handshake before starting exchanging data. Examples of protocols that use a handshake are TCP and TLS.

The TCP handshake is simple and involves three packets with the SYN, SYN-ACK and ACK flags activated. It is used to negotiate initial parameters such as the sequence numbers.

The TLS protocol also involves a handshake and it starts with a "client hello" and a "server hello" messages. The handshake is to negotiate the version of the protocol, the ciphers and random numbers that will be used to generate a secret key.

2.1.7 Address Mapping and ARP

At a higher level an application is identified by an IP address and a port number. In principle, the IP address identifies a unique host in the Internet and the port number identifies a particular application in that particular host. The IP address has two different parts - network and host - that can have variable size. The actual size of each part is specified by the network mask. As the IP address depends on the network that the host belongs to, it will change as the host roams from one network to the other. The IP addresses are network layer addresses and are hierarchical. They can be used by routers to send packets to the next hop towards the destination.

Since some link layer technologies such as ethernet support multiple hosts, they also need a link layer address. In the case of ethernet, such address is unique for each manufactured network interface card (NIC) and it is also known as a hardware address. It is necessary to have some mechanism to translate from IP addresses to HW addresses.

The link layer receives IP packets from the network layer. If the IP belongs to the same network, the packet will be sent directly to the destination. Otherwise, the packet will be sent to the next router (for example the default gateway). In a typical LAN/WLAN setting, IP address of the next hop is provided by either the IP configuration or the routing table In any case, the link layer needs to know the hardware address of the next hop.

To translate from an IP address to an ethernet address, the Address Resolution Protocol (ARP) is used. For example, to find out the hardware address associated to IP 192.168.1.1 in an ethernet network, the inquiring host broadcasts a message to the whole network "Who has IP 192.168.1.1?". The owner of the address in question answers with a directed message with its IP and its hardware address.

To avoid the sending of an ARP request for every transmitted packet, the ARP information is saved for some time in the ARP cache. The link layer will first check the ARP cache and only send a broadcast message if the required information is not present in the cache.

2.1.8 ICMP

There is a particular network protocol that is used to control the network itself. This protocol is not used by regular applications to transfer data. It is used by network administrators to obtain additional information of the status of the network.

For example, a router can send a destination unreachable ICMP message if it receives a packet for which no routing information exists. A packet that is repeatedly used by network administrators is ICMP echo request. A device receiving an ICMP request will reply with an ICMP echo reply. This can be extremely useful to test if there is IP connectivity between two devices. It is also useful to know whether a particular device is running.

Finally, as each ICMP carries a unique identifier that is included in the echo reply, it is possible to measure round-trip time. The operative system often includes a ping tool that sends multiple ICMP echo packets and keeps track of the statistics min/avg/max of the round-trip-time. Ping also provides information of the number of lost packets. It is also possible to adjust the size of ping packets to see how the network behaves with packets of different sizes. All these information can provide a good description of the status of the network. Other tools similar to ping that can be used for troubleshouting an IP connection include *traceroute* and *mtr*.

Some network administrators filter ICMP packets and therefore the absence of ping does not necessarily mean the absence of IP connectivity.

2.2 LAN and WLAN

2.2.1 Local Area Networks

Local area networks can be deployed to serve a home or a building. Ethernet is the most popular technology for wired local area networks. It typically uses UTP cables to connect end hosts and speeds of 100 Mbps or 1Gbps. Current equipment is full duplex which means that these speeds can be maintained in both directions. The nominal speed is just an upper bound for the achievable speed, as there are factors such as upper layer overheads, congestion control or switching fabric limitations that reduce the actual transmission speed.

A possible option to measure the speed that is obtained in practice can be to use a file-transfer, as FTP clients typically report the download speed at when the transfer is completed. Note that the measured speed may vary for different file sizes as the TCP windows require some iterations to fully open.

In principle, direct cables are used to connect computers to switches and switches to routers. Other connections may require cross-over cables. Many modern devices implement automatic crossover and can use both direct and crossover cables for any kind of connection.

Ethernet LAN introduce little errors and delays to the communication

2.2.2 Wireless LAN

WLAN offer the possibility of local area communication without requiring wires. The IEEE 802.11 standard makes it possible to transmit data over short distances using radio waves. There are two modes of communication: Ad-hoc in which all the participants of the network behave as peers and infrastructure in which there is an access point which is the master and the rest of the stations register as clients. In infrastructure mode, the stations communicate only with the access point. To transmit data to another station, the frames are first sent to the access point that then relays the packet to the final destination.

The most usual configuration is infrastructure in which an access point forms a wireless cell to which multiple stations connect. The Basic Service Set Identifier is the hardware address of the access point. In order to extend the coverage of a WLAN it is possible to interconnect multiple access points using a wired network. All the connected access points are assigned the same service set identifier (SSID or Extended SSID ESSID) and stations can roam from one access point to the next. Access points can be configured with multiple SSIDs to offer separate networks. For example the access points of our university advertise *eduroam* and *event@upf*.

A technology called Wireless Distribution System can be used to wirelessly connect different access points to extend coverage. The performance is considerably reduced in this case.

Differently from wired networks, wireless networks use a shared medium which is prone to errors. The transmission speed can be adjusted to be able to maintain communication in the presence bad radio channel conditions. The latest equipment implements IEEE 802.11n that supports multiple-antennas (MIMO) to increase the transmission speed. In any case, wireless networks tend to be slower and more unreliable than their wired counterparts.

Even though WLAN was originally intended for local communications, they are also being used to build wireless community networks. In these networks the neighbors connect to each other typically using roof-top antennas and covering large distances. The largest community network is called guifi.net and has more than 20,000 nodes.

Chapter 3

VLAN and STP

3.1 VLAN

By default, a device connected to a switch has level-2 connectivity to all the other devices connected to that switch. Similarly, in a switched network, all the connected devices have layer-2 connectivity to other connected devices.

A broadcast message will reach all of the connected hosts and, for this reason, the layer-2 network is also called a *broadcast domain*. For example, Fig. 3.1 shows a switched network that is a single layer-2 domain.

There are situations in which it is required to partition the network. For example, in a campus university it might be necessary to keep wireless access points in a network separated from the servers. If the access points are separated across multiple buildings, it would be necessary to have a switch for the access points in each building. Similarly, if there were servers in multiple buildings, it would also be necessary to place a dedicated switch for the servers in each building. Requiring a switch for every network in every location is a solution that does not scale as the number of locations and networks increase. It is much more convenient to have a single switched network and then configure the switches to create virtual separate link-layer networks. This is precisely what VLANs offer. Fig. 3.2 shows an example with two VLANs in which computers A, B and C are kept in a link-layer network separated from D, E and F.

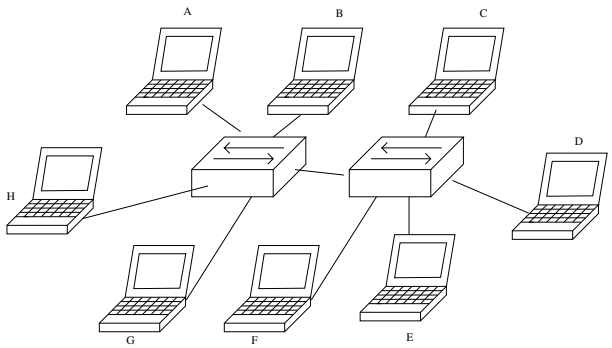

Figure 3.1: *A switched network with no VLANs.*

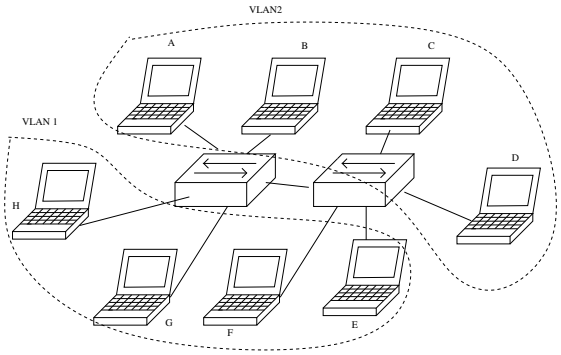

Figure 3.2: *A switched network with two VLANs*

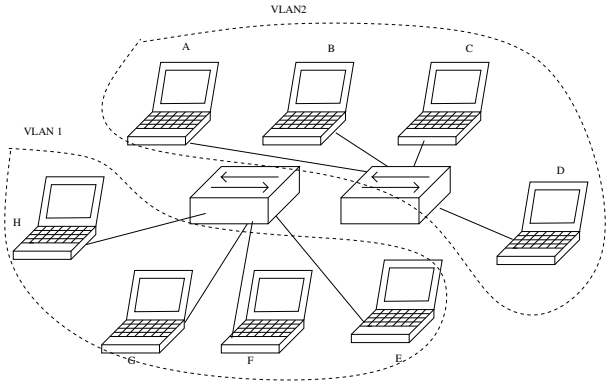

Figure 3.3: *The equivalent behaviour of the network with two VLANs depicted in Fig. 3.2*

VLANs are very convenient for deploying switched networks as it is possible for the network administrators to install a single switched network. This network can later be partitioned in a flexible way simply changing the configuration of the swithches. It is possible that ethernet ports in the same room belong to different virtual link-layer networks as it is also possible to have ethernet ports in different buildings connected to the same virtual link-layer network.

Another advantage of VLANs is that if an administrator wants to change a device from one network to another, it can simply remotely change the configuration of the switch. It is not necessary that the technician goes to the wiring closet to physically disconnect and re-connect a cable.

In a typical configuration, each VLAN contains one IP subnetwork, and it is connected to other subnetworks using a router. Each VLAN has a number which is the VLAN identifier. The switch ports are associated to VLAN by configuring each of the ports. If a switch has four ports and ports #1 and #3 are assigned to VLAN 10 while ports #2 and #4 are assigned to VLAN 20, then traffic flows from port #1 to #3 and the other way around, but it is isolated from ports #2 and #4. This kind of assignment of a single VLAN to a port is called *static-access*.

In a network deployment with multiple switches it is necessary to carry ethernet traffic from one switch to others. One option would be to connect a separate cable for each of the existing VLANs. This solution is not convenient for two different reasons. The first is that it requires many cables and many ports in each of the switches. The second is that a new cable has to be added each time that a VLAN is created.

The alternative is to use a single cable to interconnect two switches and use that cable to transmit frames of different VLANs. This makes the deployment and maintenance of the switched network easier. A port carrying packets of multiple VLANs is called a trunking port.

If packets of different VLANs are transmitted over the same switch, the receiving switch

needs to know to which VLAN each packet belongs to. To this end, the sending switch will mark every frame with information about the VLAN it belongs to. This mark is called a *tag* or, more technically, IEEE 802.1Q header.

In a default configuration, switches have a default VLAN that is also the management VLAN. Access through the management VLAN allows remote router configuration. Extreme care should be exercised when remotely configuring VLANs to prevent cutting the management connectivity. If this occurs, it might be necessary to physically access the switch to recover configuration.

Trunk switch ports can have a *native* VLANs. Packets that are received and not tagged are considered to belong to the native VLAN. Similarly, frames belonging to the native VLAN are not tagged when transmitted.

A switched network in which every device can reach any other device with level-2 connectivity is called a flat network topology. Every broadcast packet is received by every participating device. For performance, security or management reasons it might be a good idea to split the flat topology in two or more VLANs.

Each VLAN is a single broadcast domain. A broadcast packet by a host connected to a particular VLAN will reach all the devices connected to that VLAN. Importantly, that broadcast packet will not reach devices that are not connected to the same VLAN as the sender.

Two devices connected to the same VLAN have layer-2 connectivity and can directly exchange packets without requiring the intervention of a router. Devices connected to different VLANs need a router or layer-3 switch to exchange packets.

Another terminology used to refer to VLANs is *logical network segment* as opposed to a *physical network segment*. The former is created using configuration while the latter consists of actual physical cables.

The VLANs are created by assigning the ports of the switch to a given VLAN. There are two ways of making this assignment: static and dynamic.

3.1.1 Static Assignment

In the static assignment the network administrator assigns a particular port to a particular VLAN. The end host connected to that port will see other hosts connected to that VLAN and it doesn't need to be aware that there is a VLAN. A switch can have ports in different VLANs and VLANs can have ports in multiple switches.

By default all ports on a switch are connected to VLAN 1. To change a port to another VLAN, it is necessary to first create the other VLAN if it does not exist.

```
Switch(config)# vlan vlan-num
Switch(config-vlan)# vlan vlan-name
```

The assignment of a name to the VLAN is optional. The name, if given, must not contain blank spaces.

For example, to create VLANs for the classrooms and for the WiFi access points we use:

```
Switch(config)# vlan 3
Switch(config-vlan)# vlan classrooms
Switch(config)# vlan 12
Switch(config-vlan)# vlan wifi-access-point
```

A VLAN can be deleted issuing the `no vlan vlan-num` command.

After creating a VLAN, the ports of the switch can be assigned to that VLAN. The commands are:

```
Switch(config)# interface type module/number
Switch(config-if)# switchport
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# switchport access vlan vlan-num
```

The `switchport mode access` command configures the port as an access port, which is typically used to connect a host. Then, the `switchport access vlan vlan-num` assignst that port to a particular VLAN. This port will belong to a single VLAN and the host attached to that port will belong to that VLAN.

The commands `show vlans` and `show vlans brief` can be used to display VLAN port assignment information.

```
user@switch> show vlans

Name            Tag     Interfaces
default         None
                        ge-0/0/34.0, ge-0/0/33.0, ge-0/0/32.0, ge-0/0/31.0,
                        ge-0/0/30.0, ge-0/0/29.0, ge-0/0/28.0, ge-0/0/27.0,
                        ge-0/0/26.0, ge-0/0/25.0, ge-0/0/19.0, ge-0/0/18.0,
                        ge-0/0/17.0, ge-0/0/16.0, ge-0/0/15.0, ge-0/0/14.0,
                        ge-0/0/13.0, ge-0/0/11.0, ge-0/0/9.0, ge-0/0/8.0,
                        ge-0/0/3.0, ge-0/0/2.0, ge-0/0/1.0
v0001           1
                        ge-0/0/24.0, ge-0/0/23.0, ge-0/0/22.0, ge-0/0/21.0
v0002           2
                        None
v0003           3
                        None
v0004           4
                        None
v0005           5
                        None

user@switch> show vlans brief

                                            Ports
Name            Tag     Address             Active/Total
default         None                        0/23
v0001           1                           0/4
v0002           2                           0/0
v0003           3                           0/0
v0004           4                           0/0
v0005           5                           0/0
v0006           6                           0/0
v0007           7                           0/0
v0008           8                           0/0
v0009           9                           0/0
v0010           10                          0/2
v0011           11                          0/0
v0012           12                          0/0
v0013           13                          0/0
v0014           14                          0/0
v0015           15                          0/0
v0016           16                          0/0
```

3.2 Dynamic Assignment

The dynamic assignment of ports to VLANs requires to create an association between end devices MAC addresses and VLANs. Then, when an end device is connected to a switch, the switch queries a database to find out the VLAN to which the MAC address of the connected device belongs. Then the switch dynamically configures that VLAN to the port.

The advantage is that a user can connect to different ports and always be in the same VLAN. This can be useful for example for a person working in different offices or buildings.

3.3 Trunking

End devices are typically connected to switch ports that belong to a single VLAN, and the host does not need to know anything about the VLAN. The situation is different in connections between two switches. When two switches need to exchange traffic of two or more VLANs it can be a good idea to connect them using trunking ports. Trunking ports are also useful to connect switches to routers.

A trunking port carries traffic of different VLANs. The receiving end needs to know to which VLAN each frame belongs to. For this purpose, the sender marks sent packets including a VLAN ID field in the packet headers. This information is also called a tag. The receiver uses the tag to know tho which VLAN the packet belongs to and removes the tag. The tag will be added again if the receiving end needs to re-transmit the packet over another trunk connection. If a frame is sent to a host device over an access port, the tag is not included and therefore the host does not have any information regarding the VLAN ID.

The Catalyst switches that we use in this course have two different mechanisms to attach a tag to the frames. The first one is using Cisco's proprietary Inter-Switch Link (ISL) protocol. The second is using the standard IEEE 802.1Q protocol.

IEEE 802.1Q protocol inserts a 4-byte tag between the source address field and the frame length field in the layer-2 header. The first two bytes are the Tag Protocol Identifier (TPID) and are always set to 0x8100 to indicate that it is a 802.1Q tag. Of the remaining 16 bits, 3 of them are the priority field, 1 is the Canonical Format Indicator (CFI) and the other 12 are the VLAN ID.

Cisco switches implement a proprietary Dynamic Trunking Protocol that allow two networking devices to negotiate the trunk status of a link between the two of them. It is also possible to statically configure a port as a trunking port.

The commands to configure a port as trunk are:

```
Switch(config)# interface type mod/port
Switch(config-if)# switchport
Switch(config-if)# switchport trunk encapsulation {isl | dot1q | negotiate}
Switch(config-if)# switchport trunk native vlan vlan-id
Switch(config-if)# switchport trunk allowed vlan {vlan-list | all |
{add | except | remove} vlan-list}
Switch(config-if)# switchport mode {trunk | dynamic {desirable | auto}}
```

The encapsulation decides which of the possible alternatives to tag the frames will be used. In the case of a IEEE 802.1Q, it is necessary to configure a native vlan. This vlan will be transmitted without a tag. The same native vlan needs to be configured at both ends of the connection.

Then it is possible to configure which VLANs will be transmitted over this trunk. This configuration should be the same in both ends of the link.

And finally, there is the option to configure the mode as trunk or dynamic. In the case of trunk, the port will always be a trunk. In the case of dynamic desirable, the port will try to convince the other end to establish a trunk. Finally, in the case of dynamic auto, the port will switch to trunk only if the other end asks so.

The command `show interfaces trunk` provides information about trunking.

```
Cat3550#show interfaces trunk
```

```
Port      Mode         Encapsulation  Status        Native vlan
Fa0/17  trunk    802.1q         trunking   1
Fa0/18  trunk    802.1q         other      1
Fa0/19  trunk    802.1q         other      1

Port      Vlans allowed on trunk Fa0/17     1-4094 Fa0/18     1-4094
Fa0/19     1-4094

Port      Vlans allowed and active in management domain Fa0/17     1-3,10
Fa0/18     1-3,10
Fa0/19     None

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/17    1-3,10

Fa0/18    1-3,10

Fa0/19    None
```

3.4 Spanning Tree Protocol

In networking it is desirable to have alternative redundant path to be able to recover connectivity in the case of failure. In the layer-3, the routing protocol decides which are the best paths among the available ones. However, in layer 2 there is no routing protocol.

A switch learns in which port a host is connected when it receives a frame from that host. The source address of an incoming frame is stored in a MAC table together with the port that has received the frame. When a switch has to transmit a frame, it checks the MAC table to find the destination MAC address of the frame. If the MAC is found in the table, the frame is forwarded in the port indicated in the table. Otherwise, the packet is sent over all ports with the exception of the port that has received the packet.

Broadcast packets are also sent over all the ports with the exception of the port that has received the packet.

Creating alternative redundant connections results in bridging broadcast storms. Packets can circulate in circles in the network multiplying themselves and the MAC tables can be corrupted.

To prevent the problems that arise when adding redundancy to a switched network it is necessary to logically disable some of the links. This is the task of the Spanning Tree Protocol (STP). The STP constructs a logical tree topology on top of a network that may contain loops.

The switches running STP will not forward data packets until the logical tree topology has been built. To build the tree-like loop-free topology, the switches exchange bridge protocol data units (BPDU). The source address is the switch port MAC address and the destination address is a multicast address 01:80:c2:00:00:00.

There are two types of BPDUs:

- Configuration BPDU which are used to build the spanning tree.
- Topology Change Notification (TCN) which are issued when a switch detects that a ports goes up or down.

The fields in the BPDU are the following:

- Protocol ID (2 bytes)
- Version (1 byte)

- Message type (1 byte)
- Flags (1 byte)
- Root Bridge ID (8 bytes)
- Root Path Cost (4 bytes)
- Sender Bridge ID (8 bytes)
- Port ID (2 bytes)
- Message Age in 256th of second (2 bytes)
- Maximum Age in 256th of a second (2 bytes)
- Hello Time in 256th of a second (2 bytes)
- Forward Delay in 256th of a second (2 bytes)

3.4.1 Root Port Election

The first step towards the construction of the spanning tree is the election of the bridge. Each bridge participating in the STP has a Bridge ID which consists in two different parts: a Bridge Priority field and the Bridge MAC Address. The default Bridge priority is 32,768 (0x8000) The bridge with the lowest bridge ID will be elected as the root of the network.

When a switch joins the network it does not know other bridges and therefore believes it is the root of the tree. Only by exchanging BPDUs with its neighbours it can learn other bridges' IDs and discover who is the actual root.

The new bridge starts sending BPDUs placing its Bridge ID in the fields Root Bridge ID and Sender Bridge ID. If it receives a BPDU with a Root Bridge ID which is lower than its own, it will realize that it is not the root and will stop generating BPDUs. Instead, the bridge will relay the BPDUs that it receives.

When a bridge relays a BPDU it replaces the Sender Bridge field by its own Bridge ID but it keeps the same Root Bridge ID. A bridge receiving multiple BPDUs will relay only the one with the lowest Brige ID in the Root Bridge ID field. This way, after some convergence time, all bridges know the Bridge ID of the root bridge. At this point the root bridge is the only one sending BPDUs and all the other bridges simply relay the root's BPDUs.

A non-root bridge may receive BPDUs from the root bridge through different ports. In this case, the bridge will relay only the ones with the lowest path cost. To compute the path cost it will add the cost of the path through which the BPDU is received to the Root Path Cost field of the BPDU. The path cost of the incoming port is related to the bandwidth of that port. For example, it is 100 for 10Mbps, 10 for 100Mbps and 4 for 1Gbps. The root bridge sends MPDUs with a Root Path Cost equal to zero. The other bridges include the cumulative path cost to the root in Root Path Cost field.

This process constructs a tree that includes the paths of minimum cost to from each bridge to the root bridge. In the case of a tie, the sender bridge ID and sender port ID are used as tie-breakers.

In summary, the elements that are considered in determining the priority are:

- Lowest root bridge ID
- Lowest root path cost to root bridge

- Lowest sender bridge ID
- Lowest sender port ID

Each bridge marks the port through which it is receiving the best BPDUs as the root port. For each network segment, the port that is sending the best BPDUs is elected as the designated port. Designated and root ports are the only ports that should receive and send data frames in order to keep a tree topology and avoid loops.

3.4.2 STP Port States

The ports participating in STP can be in one of the following six states:

- Disabled: Administratively shut down. It does not transmit or receive anything and does not participate in the STP.
- Blocking: Ports that are not root ports nor designated ports. Blocking ports receive BPDUs and do not transmit anything.
- Listening: A port that is a candidate to be root port or designated port. It transmits and receives BPDUs and can move to the forwarding state (if it still a candidate) or to the blocking port (if it is no longer a candidate). If it is a candidate for 15 seconds will move to the forwarding state.
- Learning: A port that is a candidate to be root or designated port. The state similar to the listening state with the difference that it learns MAC addresses of the incoming data packets to populate the MAC table. If it is a candidate for 15 seconds will move to the forwarding state. If there is a better candidate will move to the blocking state.
- Forwarding: A root or designated port that transmits and receives data packets and also BPDUs.

3.4.3 Timers

As the BPDUs need to be transmitted across the network, the convergence of STP is slow and there are some timers to prevent that loops can appear during the convergence process.

- Hello: Interval between configuration BPDU transmissions (default 2 seconds).
- Forward Delay: Time spent in Listening and Learning states (default 15 seconds).
- Max Age: Maximum length of time a BPDU can be stored before discarding it (default 20 seconds).

3.4.4 Topology Changes

If a switch detects a change in the status of one of its ports goes up or down, it sends a notification towards the root bridge. The root bridge propagates the notification to all the network by setting the Topology Change flag in the Configuration BPDU. All the bridges receiving this notification will shorten the MAC table bridging time from its default value (300 s) to the Forward Delay value (15 s)

Hosts that are directly attached to a PC can be configured as PortFast and do not participate in the STP. They are brought up quickly and do not trigger Topology Changes modifications.

3.4.5 STP and VLANs

As a switched network can contain multiple VLANs it is necessary to decide how the STP is computed in each of them. The IEEE 802.1Q standard specifies a single STP for all VLANs. This can cause problems if, for example, the root does not belong to some of the VLANs. It also prevents taking advantage from load distribution among the different available paths.

A second alternative is Cisco's Per-VLAN Spanning Tree that creates a VLAN for each spanning tree but it is incompatible with IEEE 802.1Q.

Finally, a third alternative is Per-VLAN Spanning Tree Plus that is compatible with the other two and can be used in IEEE 802.1Q VLANs and keeps a different tree for each VLAN.

Chapter 4

Routing

Routers are layer 3 devices that forward packets between networks. The routers separate layer 2 broadcast domains.

Routers are specialized computing devices that have a CPU, RAM and ROM. Routers also have network adaptors to connect to networks. A router has two kinds of ports: network ports which are connected to networks and a console port for direct configuration.

A router performs two main tasks: keeping a routing table and forwarding packets.

The routing table is a list of destination networks combined with information about how to reach those networks. There are three ways of learning routes:

- Directly connected networks: The router can directly reach the networks it belongs to.
- Static routing: The routes are directly entered by the administrator.
- Dynamic routing: A routing protocol is used to automatically exchange routing information between routers.

There is a special route, called the *default* route, that is used when no other route is available. It can be statically configured by the network administrator or learned from other routers using a dynamic routing protocol.

It can happen that there are different alternatives to reach a particular network. In this case, a network metric can be used to pick between routes offered by the same routing protocol. Typical metrics include bandwidth, delay, hop count and cost. This metrics are used to compute routing distances and in general smaller routing distances are preferred.

It can also be the case that there are different routes that come from different routing protocols. For example, there can be static and dynamic routes, or routes from different routing protocols. In this case, an administrative distance is used for the router to choose between the different sources of information.

The lowest administrative distance, 0, is for directly connected networks. This is the one with higher priority. The administrative distance 1 is for statically configured networks. Higher administrative distances are assigned to different routing protocols.

There are two main approaches to dynamic routing:

- Distance vector: For a given destination network, each router only knows the next hop and the routing distance. This information is periodically shared with all neighbours.

- Link state: Each router informs all the other routers about all its other neighbours. Then each router has a complete map of the network and can choose the minimum routing distance routes.

4.1 Routing Information Protocol

The Routing Information Protocol (RIP) is a distance vector algorithm to compute routes. In distance vector routing, the participating routers periodically share their knowledge of the network with their neighbours. They send a list of the networks that they can reach together with the necessary cost to reach such networks. The information is exchanged using UDP packets and port 520. In addition to the periodic (also called gratuitous) messages sent periodically, a router that joins a network can request routing information from its neighbours in a request message.

The routers use the received announcements to populate a table that includes a destination network, a routing distance and a next hop or outgoing interface. In the case a router receives reachability announcements for the same network through different paths, it simply keeps the route of lowest cost. The list of neighbouring networks and costs are re-distributed to neighbouring routers.

RIP updates are sent approximately every 30 seconds and routes are timed out after 180 seconds. If a router stops receiving reachability announcements for a particular route for 180 seconds it simply assumes that the route is no longer available and deletes it from the routing table. To speed up routing re-convergence after a network change, when a router changes its routing table it immediately sends a *triggered* update. The triggered update includes only the changes in the routing table. If a destination is no longer reachable, the maximum value of the hop counter (16) is used to indicate unreachability.

As the maximum value of the hop counter (16) means that the destination is unreachable, the actual maximum number of hops in a RIP network is 15. This is often referred to as the diameter of the network. Consequently, RIP can only be used for small networks.

If a router detects that one of its interfaces goes down, it can update its routing table immediately by removing all the entries that used that particular interface and then send the triggered update. If a router goes down, there is no immediate way for its neighbours to detect the failure and they have to wait for the 180 seconds timeout to expire before updating the routing tables and sending triggered updates.

A problem of the RIP protocol is the *count to infinity* behaviour which is best understood by means of an example. Consider a router R_A that is connected to a network N and to another router R_B. R_B is connected to a third router R_C. R_A announces the network N with a cost 0 and R_B receives the announcements and announces N itself at a cost of 1. R_C receives the announcements of R_B and announces N itself at a cost 2. If R_A fails, R_B no longer receives announcements from R_A but still receives announcements from R_C saying that it is possible to reach N through R_C at a cost 2. Consequently, R_B updates its routing table to reflect that N is reachable through R_C at a cost of 3. When R_C receives the routing update from R_B, it updates its table to reflect that N is reachable through R_B at a total cost of 4. The routing updates continue until the maximum hopcount is reached and the routers finally delete the routes from their routing tables.

A partial solution to the count to infinity problem is the use of *split horizon*. When split horizon is in use, when routers receive a route announcement through a particular interface,

they do not announce that particular route in that particular interface. In our previous example, R_B would not announce N to R_A and R_C would not announce N to R_B. Even though split horizon solves count to infinity problem in our example scenario, it does not solve it in genera. In topologies containing loops, the count to infinity problem can appear even when split horizon is in use.

In addition to use split horizon, a router can explicitly say that a particular route is unreachable by sending a distance equal to the maximum hop count that is interpreted as infinite. This technique is known as route poisoning.

RIP also uses a holddown timer to prevent route unstability. When a router receives information about a route being previously previously reachable is now unreachable, the router marks the route in question as inaccessible and starts a holddown timer. Until the holddown timer expires the router will only accept route announcements about that particular route with a lower cost than the one contained in the original route. Other route announcements indicating the reachability of the networks are disregarded. Only after the holddown timer has expired, new routes with higher or equal metric will be considered and the route can be installed again in the routing table.

There are three timers that are used in RIP. The first one is for the periodic RIP updates and takes a random value between 25 and 35 seconds. A random value is used to prevent that the routers synchronize and send all the routing updates at the same time causing the congestion of the network. The second one is for timing out a route and has a duration of 180 seconds. Finally, the last one is for garbage collection and lasts 120 seconds. When a route is no longer valid, the router sends announcements with that route with a distance set to the maximum hop count which is equivalent to infinity. This helps the neighbouring routers to purge the route that is no longer valid. The holddown timer default is 180 seconds in RIP.

Compared to OSPF, RIP is simpler. The drawbacks of RIP are that it places a limit in the maximum cost between two networks to be 15 and it is slower to converge and to react to changes. Furthermore, RIP has severe limitation when it comes to assigning costs to a link. It is possible to assign a link cost higher than one, but it reduces the maximum number of hops in the network as the maximum allowed cost for a reachable route is 15.

4.2 A Cisco Router

When a cisco router boots, it goes through a power-on self test (POST), then it loads the Internetworking Operative System (IOS) and finally loads the configuration. You can connect to the router using the console port and a serial port terminal such as Hyperterminal for windows or gtkterm for linux. Once you are connected to the router, there are two main modes of operation: user mode and privileged mode. The first one allows you to check the router status while the second one is for changing the router configuration. The `enable` command can be used to enter the privileged mode. When in privileged mode, the prompt shows a hash sign (`#`).

The question mark (`?`) can be used to know which commands are available. It can also be used in the middle of a command for help information about how to continue.

The `show version`, `show running-config` and `show` commands can be used to obtain additional information about the router. To enter the global configuration mode you can use the command `configure terminal` or, equivalently, `conf ter`. The global configuration mode is indicated in the prompt as `config`. It is possible to access the specific configuration modes from this point. For example, the command `interface serial 0` can be used to go to the interface specific configuration mode for the Serial 0 interface. To move back to the previous mode, the exit command or the Ctrl-Z shortcut can be used.

To enter into the router specific configuration mode we can enter, for example, the `R1(config)#router`

`rip` command and then the `R1(config-router)#network 10.0.0.0` to include a particular network in the routing process.

To other particularly relevant commands for routing are the `show ip protocols` and the `show ip route` commands.

Chapter 5

Firewall and Network Security

Protecting information can be more complex than protecting phyisical goods. We may be interested in preventing that information can be duplicated or read by third parties. We may want to also protect information from being modified or erased.

The internet makes it possible for the information to easily travel accross the globe. All the protocols and tools that are typically used with good intentions can also be used to abuse and exploit information systems. Therefore, it is important to keep security in mind when designing and managing information networks.

Security can be present at different layers of the protocol stack. For example, the TLS protocol offers security at the application layer in the internet protocol stack. TLS is used to protect HTTP sessions in the HTTPS protocol. The open source implementation of TSL OpenSSL was recently in the news after the heartbleed bug was discovered.

IPsec offers security at the network layer. It can be used to protect all traffic between two endpoints. These endpoints can be either a host or a network. IPsec uses two different forms of protection. The Authentication Header (AH) provides integrity, data origin authentication and protection against replay attacks. The Encapsulating Security Payload (ESP) header provides confidentiality, data origin authentication, integrity and protection against replay attacks.

IPsec can operate in two different modes: transport mode and tunnel mode. In the first one, the payload of an IP packet is protected while the IP headers are left unmodified. In the second mode of operation, IPsec tunnel mode, the entire IP packet is protected and encapsulated within a new IP packet.

Another aspect of security is access control and network perimeter protection. It is desired to prevent unauthorized access to computers and networking devices. In the internet there are automatized tools that are continuously looking for vulnerabilities to gain unauthorized access to systems. Botnets are hordes of infected computers (also called zombies) that follow the commands of a master and can be used to send spam, perform port scans, or search for vulnerable systems.

Keeping the software updated and using strong passwords helps in keeping systems secure. Another tool that helps in protecting networks and computers are firewalls. Firewalls filter traffic and stop undesired and potentially malicious packets. The firewall can be installed in an end computer, to protect only that computer, or in a networking device to protect a network.

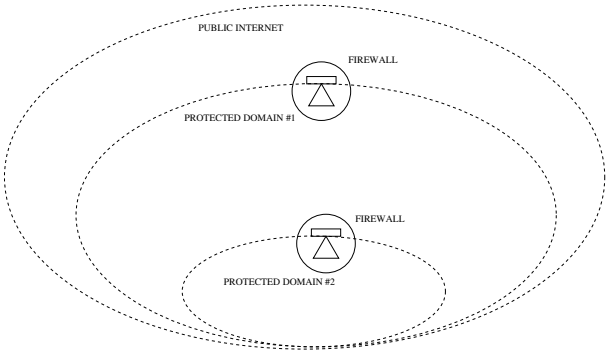

Figure 5.1: *Nested security domains.*

We will be focusing on the latter kind of firewall.

5.1 Firewall

A network can be protected from attacks coming from the rest of the internet by placing a firewall in the frontier between the two networks. To be effective, it is important that all the traffic exchanged by the network and the rest of the internet goes through the firewall. The firewall filters undesired traffic to offer partial protection against external attacks. Note that a negative aspect of forcing that all the traffic between our network and the internet is handled by the firewall is that it introduces a single point of failure. It is possible to have two firewalls with the same configuration to mitigate this problem.

In perimeter protection, networks are called security domains and are classified regarding their level of trust. For example, the network of the organization can be considered trusted and therefore it is a trusted security domain. The public internet can be considered untrusted and it is therefore an unstrusted security domain. A firewall is placed between the two of them to enforce access control rules. The firewall protects the trusted domain from the unstrusted domain.

More complex topologies are possible. For example it is possible to have multiple nested security domains with multiple firewalls securing each of them. In this case, the network that is considered trusted by one firewall is considered untrusted by another firewall. This situation is illustrated in Fig. 5.1.

Another common situation is that an organization wants to expose some information to the internet, for example using web servers. This web servers need to be placed in a network that can be accessed from the outside. It is still possible to offer partial protection to this servers using a firewall. For example, the firewall can be configured to allow only web traffic between the internet and the network of the web servers. This partially protected network is typically named DMZ (for demilitarized zone). The organization can keep a network totally protected (internal) and another network partially protected (DMZ), as shown in Fig. 5.2.

There are two possible options to separate the trusted and untrusted domains. The first one is physical separation, in which the two domains use different hardware. The second option is logical separation, in which the two domains share some hardware and are logically separated using VLANs or MPLS tags. Physical separation is considered safer than logical separation.

5.1.1 Chain of rules

There are also to different approaches when configuring a firewall: Permissive access control (reactive) and restrictive access control (proactive). In the first one, traffic is allowed unless

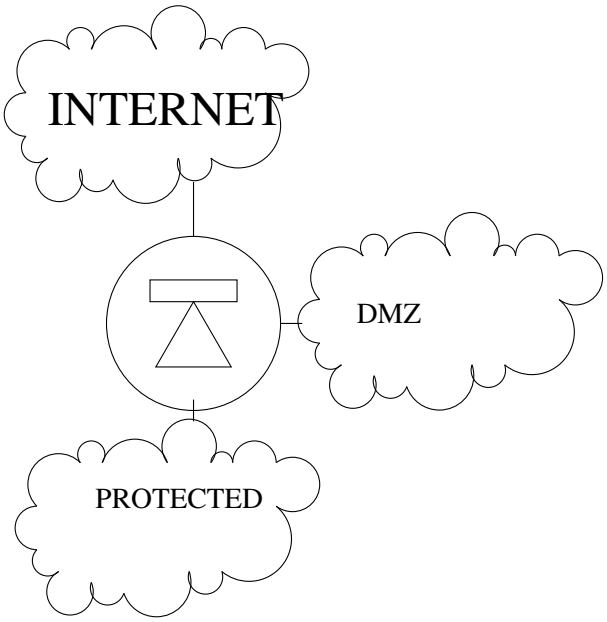

Figure 5.2: *The firewall separates the public internet, the protected network and a DMZ.*

explicitly forbidden. If a threat is detected, the network administrator adds a new rule to the firewall to protect the network from the threat. In restrictive access control, the traffic is forbidden unless explicitly allowed. When a new service requires to send packets through the firewall, the network administrator adds new rules to the firewall to permit the traffic associated to the new service.

A firewall is typically implemented as a chain of rules that are checked one by one until one of the rules matches. When there is match, the rule has an associated action that can be either allow or deny. In the case of a restrictive firewall the last rule of the chain denies (rejects) all traffic that does not match any of the previous rules. In a permissive firewall, the last rules allows any traffic that has not been dropped by any of the previous rules.

The following listing shows an example of a restrictive set of rules:

```
Src              Dst     Protocol        Service            Action
192.168.1.11/32  any     tcp             80                  Allow
192.168.1.0/24   any     any             any                 Drop
any              any     udp             53                  Allow
any              any     any             any                 Drop
```

The rules chain applies to a particular interface and a particular direction of traffic.

5.1.2 Stateless Firewall

In its simplest form, a firewall takes decisions based uniquely on the headers of the packet. This information can include information regarding IP addresses, layer 4 protocol and ports. For example, a firewall allowing only packets to and from a particular host could be implemented as a stateless firewall. A firewall that allows all packets that use port 80 as a source or destination port could also be implemented with a stateless firewall.

5.1.3 Stateful Firewall

Consider the previous example of allowing all packets that contain port 80 as either its source or destination port. This configuration allows the computer in the protected network to browse the

web available in servers of the public internet. A problem with this configuration is that any host of the public internet can access any computer and any port in the protected network by simply using port 80 as its source port. This configuration gives little protection to the protected network.

An alternative to allow the computers in the protected network to visit web browsers in the public internet while keeping the protected network more secure is to use a stateful firewall. The stateful firewalls keeps the state of a connection and can take a decision about whether to allow or reject a packet taking into account the history of packets that have traversed the network before. When a client in the protected network sends a packet to a web server in the public internet, the firewall stores the addresses and ports of this packet in a database and then will allow the packets that are answering this particular request. Compared to the stateless firewall that accepted all packets that used port 80, the stateful firewall accepts only those packets that are answering a request initiated in the protected network. Stateful firewalls are much more effective and therefore are the firewalls that we normally use nowadays.

5.2 Related Security Concepts

5.2.1 Deep Packet Inspection

Normal firewalls consider only information available in the network layer and the transport layer of the packet. Deep packet inspection (DPI) is about re-constructing application layer messages and taking decisions based on this information. A deep packet inspection firewall can differentiate between a web packet and file sharing packet even if they both use exactly the same IP and port information. A DPI can be much more precise in making decisions thanks to the additional information it has access to.

The problem is that the number of applications is very large and is growing continuously. It is difficult to keep track of all existing applications. Furthermore, looking into the application messages and interpreting application information is computationally expensive and consumes CPU time. Therefore, the packet processing speed is much lower for DPI than it is for normal firewall operation. Some applications encrypt the information making it more difficult or impossible for the DPI firewall to extract information from the application layer.

5.2.2 Intrusion Detection and Prevention Systems

An intrusion detection system (IDS) is a device or software that continuously monitors network traffic to detect anomalies that can be indicative of an attack. We can differentiate to kinds of IDS:

- Signature-based: The IDS has a database of signatures of virus and malicious packets in general. The IDS continuously compares the network packets with the signature database and rises an alarm when malicious packets are detected. It is important to keep updating the database as new attacks are discovered.

- Statistics-based: The IDS gathers statistics about *normal* traffic behaviour. Then, it continuously compares traffic statistics with what is considered normal and rises an alarm when it detects abnormal traffic patterns.

IDS have the problem of issuing false positives and false negatives. In a false positive event, an alarm is raised when there is no attack situation. In a false negative event, an attack goes undetected.

An intrusion prevention system (IPS) is an IDS that has the capability to automatically take action to prevent the attack. An IPS can, for example, change the firewall rules to stop malicious traffic.

5.2.3 Application Layer Gateway

An Application Layer Gateway (ALG) works in combination with a firewall to interpret messages at the application layer as in DPI. An ALG uses the information to adjust the firewall rules or to rewrite the message to allow legitimate user communication through the firewall. The ALG is intended for protocols that open additional ports to perform their task, such as SIP, FTP and BitTorrent.

5.3 Network Address Translation and Port Address Translation

Network address translation (NAT) translates addresses between two domains. When the protected domain uses private addresses, NAT is required to translate those addresses to public internet addresses.

5.3.1 Static mapping NAT

In its simplest form, NAT is a one-to-one mapping. For example, private address 192.198.1.1 could be translated to a public address 193.145.56.1. This translation can be bi-directional, and all packets arriving at the public-facing interface can be translated to the corresponding private address. With this kind of mapping, a client in the public internet can contact a server in the private IP addressing space if it knows the corresponding public address.

5.3.2 Dynamic mapping NAT

In a more complex situation, several devices on the private address space share a set of public addresses. In this situation, the NAT device dynamically uses public addresses for translating the private addresses. The NAT device can take advantage of statistical multiplexing. If the devices with private address are not always online, it is possible to use a set of public address to serve a larger number of devices. The same device will probably be mapped to different public IP addresses at different times. As this is no longer a one-to-one correspondence, it can be more complicated to host a server using the private address space its public equivalent address it is not always the same.

Despite the fact that in general there is not a one-to-one mapping between private and public addresses, if we look at any particular time instant there is a one-to-one mapping between those private addresses that are active and the public addresses. The difference with static NAT is that in static NAT this one-to-one correspondence is valid for any period of time, while in dynamic NAT the one-to-one correspondence is valid only for a particular instant and can change dynamically. The devices in the private address space take turns in using the public addresses, but they do not use them simultaneously.

The number of devices with private addresses that can simultaneously access the public internet is limited by the size of the pool of available public addresses.

5.3.3 Port Address Translation

Port address translation (PAT) allows that different devices with private addresses simultaneously use the same public address. In NAT/PAT, both IP addresses and port numbers are translated.

The NAT/PAT device keeps a database with the association of address and port in the public side and the private side. Each entry in the database has four fields: original address, original port, translated address and translated port. Two different private addresses can be translated to the same public address as long as the resultant translation has different ports and therefore the translated address and translated port tuple is unique.

If two devices in the private network send a web request to the same webserver, the two packets will have different source addresses in the private network. When this packets are translated by the NAT/PAT device, they will have the same source and destination address, but they will have different source ports. The two reply answers from the webserver will have the same source and destination ports and different port destination number. When receiving the two answers, the NAT/PAT device will differentiate the two packets using the different destination ports. In the database in the NAT/PAT device there will be stored the private addresses that had originally initiated the web requests. The NAT/PAT device will translate the two packets coming from the webserver using the two different addresses in the database and send the reply packets to the two devices that had originated the request.

PAT is also known as masquerading.

In principle, it is not possible for a client in the public internet to access a server in the private network unless port forwarding is used.

5.3.4 Port Forwarding

PAT is very useful when the number of public addresses available is limited and also to hide internal network topology. Still, there are occasions in which is desirable to host a server in the private network behind the NAT/PAT. If it is not possible assign a public address to the server in the NAT/PAT device, an option is to assign it an address and port tuple. When the NAT/PAT device receives a packet in the public-facing interface that is directed to specified address and port tuple, it applies a static translation rule and directs it to the server behind the NAT/PAT.

For example, in a private network with a SMTP server and a web server installed in different hosts and with different private addresses, it is possible to install static rules in the NAT/PAT device that redirects some traffic arriving to the NAT/PAT public interface to the appropriate server. In particular, there will be a rule that redirects traffic with destination port 80 to the webserver and with destination port 25 to the email server.

Part

II

Lab Sessions

Chapter 6

Traffic Analysis

6.1 Introduction

The goal of this lab assignment is to learn about monitoring and traffic analysis tools. We shall use the *Wireshark* and *tcpdump* software tools to study different layers of the TCP/IP architecture.

Important
For this practical exercise, you have to submit a report the answers to the questions below. When submitting the answers to the questions, be brief but precise. If you include screenshots, indicate on the screenshot what is the answer.

6.2 Home Preparation

Review the TCP/IP model and explain the function of each layer. Provide examples of the protocols at each layer of the protocol stack.

Questions and Tasks ($7 \times 2\,\%$)
What is the purpose of ARP? Tip: Use the RFC826 standard to answer this question [**?**].
Draw a sketch of the different messages being exchanged and the different steps involved.
Is it possible to run this protocol between computers that are in different local area networks (LANs)?
What is the ICMP protocol?
How does the ping command work?
What does the ping command measure? Include at least two items.
Explain and draw an SSL connection indicating how the protocol works and which messages are being exchanged.

6.3 Disable Your Local Firewall

On a Windows machine, your local firewall can interfere with the assignment. Go to the Control Panel, Windows Firewall and from the left-hand site options list, select Turn Windows Firewall on or off. In the page, select the option Turn off Windows Firewall (not recommended) for both private and public networks, and then click OK.

6.4 Wireshark Network Analyzer

Start your computer in Windows or Linux. Start the *Wireshark* software program and choose the correct network interface from the Capture >Interfaces dialog. Use it to start the packet capture. It is also possible to configure the length of the capture and other details.

Question (2 %)
What interfaces does Wireshark detect? What is your IP address? What is the corresponding MAC address?

Configure the Capture >Interfaces options to perform a capture of a few minutes. Observe the results and answer the following questions.

Advice
You may stop the capture when you have received a reasonable number of packets.

Question (2 %)
What is the total number of captured packets? Are there lost packets? If yes, why? Include a screenshot of the Wireshark window, indicating from where you determined this information.

Select one (any) packet. Observe the details and answer the following questions, including for all answers the summary of the packet with the description of each layer protocol, as in the following example.

```
? ?.????????? 10.80.26.113 173.194.34.243 HTTP 1704 GET / HTTP/1.1
Frame ?: 1704 bytes on wire (13632 bits), 1704 bytes captured (13632 bits) on interface 0
Ethernet II, Src: G-ProCom_c8:f4:5c (00:0f:fe:c8:f4:5c), Dst: Cisco_00:0a:01 (00:07:b4:00:0a:01)
Internet Protocol Version 4, Src: 10.80.26.113 (10.80.26.113), Dst: 173.194.34.243
  (173.194.34.243)
Transmission Control Protocol, Src Port: 53744 (53744), Dst Port: http (80), Seq: 1, Ack: 1,
  Len: 1650
Hypertext Transfer Protocol
```

Questions (6 × 2 %)
What is the source and destination IP address?
What are the source and destination MAC addresses?
What is the number of bytes in the packet?
What protocols can you see in the packet?
Did you capture an HTTP packet? If yes, what is the length of the HTTP message (that is payload of the TCP segment or segments)?
What are the source and destination port?

In the dialog Analyze >Enable Protocols... you can configure the protocols that Wireshark captures and displays. Looking at the default protocols, find at least one protocol of each of the four upper layers of the TCP/IP stack (application, transport, internet and link). Include a brief description of the protocols you found.

Select the menu Statistics >Protocol Hierarchy and observe the percentage of the following protocols: Ethernet, Internet Protocol, TCP, UDP, Logical Link Control, ARP, STP, IPv6, HTTP.

Repeat the previous capture using IPv6, by performing a ping to the local-link IPv6 address of a neighbor computer. Use the following command on a Windows computer:

```
ping -6 <destination-address>
```

or the following command on a Linux computer:

```
ping6 -I <interface> <destination-address>
```

Question (2 %)
What are the protocol differences between IPv4 and IPv6?

6.5 The Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) resolves the association between an IP address and a MAC address. It is used in IP over Ethernet networks. Clear your ARP cache using one of the following commands. On a Windows computer use:

```
arp -d
```

On a Linux computer use:

```
sudo ip neigh flush all
```

Begin a new traffic capture and then ping or browse to any preferred destination. Analyze a pair of request-response ARP packet. You can filter the ARP packets by writing `ARP` in the Filter Toolbar.

Questions (4 × 2 %)
What are the source and destination MAC addresses of the Ethernet frame that contains the ARP request message? The response should state in words the meaning of the MAC addresses, not their values.
What are the source and destination IP addresses in the ARP request and response frames? The response should state in words the meaning of the IP addresses, not their values.
What are the source and destination MAC addresses in the ARP request and response frames? The response should state in words the meaning of the MAC addresses, not their values.
What is the time elapsed between an ARP request and reply messages?

Use the information available in *Wireshark* to indicate the length of the ARP frames and draw the format of the messages.

Question (2 %)
To which layer does ARP belong?

6.6 HTTP and Secure HTTP

Begin a new capture of a few minutes and during this time visit a few web sites, such as `http://www.upf.edu` and `https://www.google.com`. After the capture finishes, observe the HTTP and HTTPS messages by typing `http or ssl` in the filter toolbar. Observe an HTTP GET message and the corresponding response and answer the following questions.

Advice
You may stop the capture when you have received a reasonable number of packets.

Questions ($5 \times 2\,\%$)
What is the HTTP version of your web browser?
What is the HTTP version of the server?
What language does the client request to the server?
Is it possible to find which are the URLs visited by the user?
At which layer is this information available?

The default destination port for web is 80 or 8080, when using a web proxy.

Questions ($2 \times 2\,\%$)
What is the source port of the GET requests?
Write the source port number for different connections. At which layer can you find this information?

Find a DNS query–response message pair. Use `dns` in the *Wireshark* filter.

Question (2 %)
What is the function of DNS?

Use the option Analyze >Follow TCP Stream to analyze a TCP session. Identify the three-way handshake and the session tear-down.

Question (2 %)
When using HTTP, it is possible to observe the contents of the web using Wireshark?

Now use HTTPS.

Question (2 %)
Is it still possible to read the information that is being transmitted? Tip: Search for SSL packets.

Identify a SSL handshake in *Wireshark*.

6.7 ICMP Ping Packet Capture

Close all applications that use the network and `ping` four different web sites on four different continents, as indicated by your instructor. Analyze the results.

Question (2 %)
What are protocols used?

Draw a frame and explain how the different packet are encapsulated in each other.

Question (2 %)
How many ping messages are transmitted by default?

Prepare a table with the source, destination, and average packet delay of the four different ping experiments.

Questions (8 × 2 %)
What is the packet length?
At which layers can we find source and destination addresses?
What are the addresses types?
Are the ping ICMP query packets sent at constant time intervals in time?
What about the ICMP replies?
What are the reasons for different inter-arrival times for the ICMP reply?
What information is included in the data field of the ICMP packets?
What about in the reply messages?

6.8 `tcpdump`

In this section, we shall use the `tcpdump` command in Linux. Use:

```
man tcpdump
```

to learn about the different parameters and options of this command. With `tcpdump` it is also possible to filter the traffic according to the source or destination addresses, protocol, port number, etc.

Open a terminal and begin a new `tcpdump` capture. Enter the Ctrl+C keys to finish the capture.

Questions (2 × 2 %)
What is the information provided by `tcpdump` and what is the format used?
With the default options, to which network layer does the information belong? Tip: Remember that you can redirect the output to a file using the following command `tcpdump >file_name`.

The first line of `tcpdump` specifies the network interface used during the capture. To change it, use the `-i` option.

Question (2 %)
What is the interface that you are using?

Describe the information provided for the ARP protocol using the following command.

```
tcpdump arp
```

Then, execute the same command again using the `-e` option.

Question (2 %)
What is the difference with respect to the previous execution? Tip: Use the `tcpdump` manual, if necessary.

Run a `tcpdump` capture for each of the following cases. In each case, find the corresponding filters that you must add as parameters to the `tcpdump` command.

Questions (5 × 2 %)
Run a capture only for IPv4 and IPv6 packets. What are the command filters?
Run a capture only for IPv4 packets originating at a specific IP address. What is the command filter?
Run a capture only for UDP packets. What is the command filter?
Run a capture only for STP packets. What is the command filter?
Run a capture only for HTTP and HTTPS packets. What is the command filter?

Chapter 7

LAN and WLAN

7.1 Home Preparation

Important

For this practical exercise, you have to submit a report the answers to the questions below. When submitting the answers to the questions, be brief but precise. If you include screenshots, indicate on the screenshot what is the answer.

Connect to the web configuration interface of your home access point.

Questions ($3 \times 1.5\,\%$)

What are the range of frequency channels available for your access point?

What are the physical layer data rates supported by your access point?

What are the security protocols supported by your access point?

Perform a survey and find the information of available wireless networks. On a Windows computer, you can use the following command:

```
netsh wlan show networks mode=bssid
```

On a Ubuntu computer, you can use the following command:

```
sudo iwlist <wlan-interface> scan
```

Task (5.5 %)

Add the survey to your report, including the following information for each network:

- the network name (SSID or ESSID)
- radio type
- radio channel
- physical layer data rates
- security settings

7.2 Equipment

Each group requires at least *two* (2) or *three* (3) computers. Start one computer in Windows and the other one in Ubuntu. The hardware we shall use during this lab is the *Cisco Aironet 1200* access point. The firmware of the access point is *CISCO IOS Version 12.3(8)JA2*, and you can download the corresponding at the following link:

`http://www.jaumebarcelo.info/teaching/lxs/wlan/WLAN_manual.pdf`

To test copying a file across the wireless network, install an FTP server on one of the computers, such as *Filezilla* in Windows and *vsftpd* in Ubuntu. You may use a web browser as an FTP client.

- On Windows, install and open *Filezilla*, and connect locally from the same PC using the *loopback* interface 127.0.0.1. Create a new user (username `test` and password `test`) and share a local folder with several large files. Do not forget to remove the proxy configuration, or select not to use a proxy server for local addresses.
- On Ubuntu, install *vsftpd* with the following command:

```
sudo apt-get install vsftpd
```

  Once installed, you can find and modify the FTP server configuration in the file `/etc/vsftpd/vsftpd.conf`. If you need to change the configuration, do not forget to restart the FTP server with the command:

```
sudo services vsftpd restart
```

  The server allows by default anonymous access, and therefore you do not need to create a new user. The default shared folder is `/var/ftp`.

7.3 Disable Your Local Firewall and Pay Attention to Your Browser

Your local firewall can interfere with the assignment. Disable the firewall on both Windows and Ubuntu computers. On a Ubuntu computer, you can disable it using the following command:

```
sudo ufw disable
```

Important

We recommend using Internet Explorer to interact with the access point web interface. If you decide to use Firefox to connect to the access point during the assignment, it might be necessary to disable the proxy settings and to uncheck the offline navigation option.

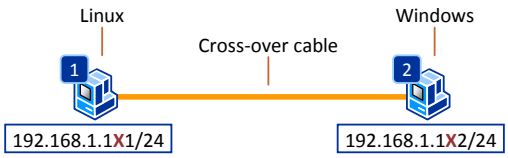

Figure 7.1: *The network topology used for the LAN exercise.*

7.4 Basic LAN Configuration

Connect the Windows and the Ubuntu computers using a cross-over cable, as shown in the figure 7.1. Configure the interfaces with an IPv4 address if needed. Check layer 2 connectivity using the LED or the `ethtool` command in Ubuntu. Check layer 3 connectivity and measure round-trip time using `ping`.

Next, you need to estimate the available bandwidth using an FTP file transfer or the `iperf` tool. You must select a file of at least 100 MB or larger. Change the Ethernet connection speed to 10 Mbps (full duplex) and estimate the bandwidth again.

On a Windows computer use the configuration of you network interface card to change the speed. On a Ubuntu machine, you can check your Ethernet interface configuration using the command:

```
ethtool eth0
```

and change the configuration:

```
sudo ethtool -s eth0 speed 10 duplex half
```

After testing, remember to change the configuration back:

```
sudo ethtool -s eth0 speed 1000 duplex full
```

Task (10 %)

Include a brief report of your activity, which must include the following information:

- the selected speed for the network interface of each computer
- the size (in bytes) of the file you transferred using FTP
- the download duration

Questions (2 × 5 %)

What is the average file transfer speed that you obtained for the file download in each instance?

Does the transmission speed reach the physical layer bandwidth? Why do you believe this is so?

7.5 WLAN Basic Configuration

WLANs can be used as an access point (AP) to LANs. They can also be used to interconnect to LANs using wireless distribution system (WDS). WDS can also be used to extend the coverage of a WLAN with access points that do not have a wired connection. IEEE 802.11 headers can accommodate up to 4 addresses to differentiate between final addresses and per-hop addresses[1].

[1] This is explained in the theory session

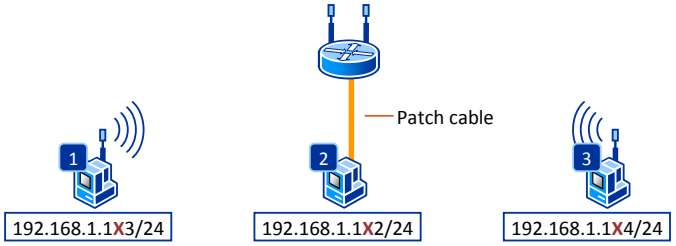

Figure 7.2: *The network topology used for the WLAN exercise.*

Connect the access point to the Windows computer as shown in the figure 7.2. You may use either a direct connection or a connection using the patch panel. Use the Internet Explorer browser to connect to the access point web interface. The IP address is available on the access point, and the administrator user is `Cisco` and the password is `Cisco`.

Go to the Express Security page and configure the access point with the following settings, where X is the number of your group.

Setting	Value
SSID	`LAB-XIS-X`
Broadcase SSID in Beacon	Selected
VLAN	No VLAN
Security	No Security

Go to the Network Interfaces >Radio0-802.11G page and enable the radio interface of the access point.

Install a wireless interface in the Ubuntu computer from the previous exercise, and, if available another wireless interface in the third computer. Connect both computers with a wireless interface to the access point that you have just configured. Check that you have network connectivity and use the `ipconfig` (on Windows) or `ifconfig` (on Ubuntu) commands to look at the interface configuration. If you have network connectivity, you should be able to ping the other computers of your group (both with wired and wireless connections).

Tasks ($3 \times 5\,\%$)
Measure the throughput using FTP to transfer a large file from the wireless computer to the wired one and the other way around. Include a brief description (a few sentences) of your activity.
Measure the round-trip-time using ping. Include a brief description (a few sentences) of your activity and of the obtained round-trip time.
Use either the `netsh` or `iwlist` commands to detect the available wireless networks. Include in your report their configuration.

Questions ($3 \times 5\,\%$)
Can you reach the physical layer rate maximum throughput? Why do you believe this is so?
Do you observe the same values for the uplink and downlink? Tip: Perform several experiments in each direction to confirm the measurements.
If the throughput values for the uplink and downlink differ significantly, why do you believe this is the case?

Advice

Discuss with the your instructor the interpretation of your results.

7.6 Hot-Standby

Important

For this assignment you must collaborate with another group. Ask for the assistance of your instructor before you begin setting up your access point.

The hot-standby is a feature to offer high availability. It consists of a backup access point (*AP-standby*) which takes over if the primary AP (*AP-root*) fails. One group will configure the *AP-root* and the other the *AP-standby*. Before you begin disconnect all wireless computers from your access point.

Important

Make sure that you have the same configuration (with the exception of the IP address) on both access points, including the network SSID, network mask and security setting. Ask for the assistance of your instructor if needed.

Go to the Express Security page and configure the access point with the following settings, where X and Y are the numbers of the two groups.

Setting	Value
SSID	`LAB-XIS-XY`
Broadcase SSID in Beacon	Selected
VLAN	No VLAN
Security	No Security

- In the *AP-root*, go to Network Interfaces >Radio 802.11g, and select Access Point (Fallback to radio shutdown).
- In the *AP-standby*, go to Services >Hot Standby. Select Enable and specify the MAC address that the AP will be monitoring (the radio interface of the root-AP). If the configuration is correct, you should be able to see the status that will appear below on the screen.

Connect a wireless computer from each group to the new wireless network that you just configured. Test the wireless connection using the `ping` command from each wireless computer to the other. If you are using a Windows computer, run the command continuously using the `-t` switch.

Tasks ($2 \times 4\,\%$)

Draw a sketch of the involved network devices and connections and include it to your report. The sketch must include the MAC and IP addresses of all network interface cards, and of the access point.

Use the Home page of the access points to determine to which access point are the two computers connected. Include a screenshot of this list to your report.

Test the standby functionality, by disabling the radio interface of *AP-root* from Network Interfaces >802.11g >Settings. After the time-out expires, the AP-standby should take over with the same SSID and security settings.

Tasks (2 × 4 %)
Confirm that the two wireless computers connected to the AP-standby by including the output of the `ping` command and the log from the Home page of the AP configuration interface to your report.
Use the Home page of the access points to determine to which access point are the two computers connected. Include a screenshot of this list to your report.

Questions (2 × 2 %)
How long does it take for the computers to recover the connection after the AP-root's radio is disabled (your best estimate)?
Will the user notice that the connection switches from one AP to the other? How?

7.7 Configuring an AP as a Repeater

A repeater AP is not connected to the wired LAN. It is situated within the coverage range of another access point to extend the covered area. Similar to the previous exercise, both access points must share the same configuration (with the exception of the IP address). In this exercise, we shall use the previous *AP-standby* as a repeater.

Before you begin, disconnect your wireless computers from the access point.

- In the *AP-root*, go to the Network Interfaces >802.11g >Settings page and for the option Role in Radio Network select Access Point.
- In the *AP-repeater* (the former *AP-standby*) disable the hot-standby option. Go to the Security >SSID Manager page and at the bottom of the page for the option Guest Mode / Set Infrastructure SSID >Set Single Guest Mode SSID select the current SSID. In the Network Interfaces >802.11g >Settings page for the option Role in Radio Network choose Repeater.

After you have completed the configuration on both access points, connect a wireless computer from each group to the new wireless network that you just configured. Test the wireless connection using the `ping` command from each wireless computer to the other. If you are using a Windows computer, run the command continuously using the `-t` switch.

Initially, the client computers are probably connected to the *AP-root*. The Home page from each access point should show the configuration of your network, including the repeater and any connected clients. By selecting the Clients options, you will see the list of associated clients.

Task (6 %)
Include a screenshot of the network configuration from each access point in your report.

On the *AP-root*, de-associate a client computer, in which case the client will automatically re-connect to the repeater. After the configuration changes have been completed, your home screen should show the configuration of your network and the repeater, and the clients connected to each AP.

Tasks ($2 \times 7\,\%$)
Include a screenshot of the updated network configuration from each access point in your report, after you de-associated a client and the client reconnected to the other access point.
Include the output of the `ping` command to your report to confirm the the de-associated computer reconnected successfully to the other access point.

Chapter 8

Virtual Local Area Networks (VLANs)

8.1 Home Preparation

Important
For this practical exercise, you have to submit a report the answers to the questions below. When submitting the answers to the questions, be brief but precise. If you include screenshots, indicate on the screenshot what is the answer.

You can download the switch user manual from here:
http://www.jaumebarcelo.info/teaching/lxs/wlan/manual_vlan.pdf

Questions ($5 \times 3\,\%$)
What is a VLAN and what is used for?
What are the differences between the different modes of the Cisco IOS command-lien interface (CLI)?
How do you establish a relationship between the active VLANs and the different ports of the switch?
What are the differences between access ports and trunk ports?
If you have two switches, include and explain at least three (3) different connectivity situations.

8.2 Introduction

In this lab assignment, we shall configure a Cisco switch to create different VLANs. Your instructor will give your the IP addresses of the lab switches, which shall be similar to the ones from the table below. During this assignment, each group of students will be assigned to a switch. Before you begin, you must connect the Ethernet cable of your computers to the switch assigned to your group, in the manner indicated by your instructor.

Each VLAN has a unique identifier that takes values between 0 and 4094. In this lab assignment we shall use the identifiers *10* and *20*. Each group will use *three computers*. With one computer you shall manage the switch, and this compute requires an IP address in the same

Student Group	Switch	IP Address
Group 1	Switch B	192.168.1.102
Group 2	Switch C	192.168.1.103
Group 3	Switch D	192.168.1.104
Group 4	Switch E	192.168.1.105
Group 5	Switch F	192.168.1.106

Table 8.1: *The IP addresses of the lab switches (subject to change, according to the instructions received during the lab).*

Student Group	Computer	IP Address
Group X	Computer using VLAN 1	192.168.1.20X/24
Group X	Computer using VLAN 10	192.168.10.X/24
Group X	Computer using VLAN 20	192.168.20.X/24

Table 8.2: *The IP addresses of the computers.*

subnetwork as the address of the switch. Your instructor will give your further details. The IP addresses of the other two computers must belong to the range of the VLAN that you are going to use, as shown in the table 8.2.

8.3 Creation of a VLAN

All Cisco switches used during this lab, use an operating system called the Cisco *Internetwork Operating System*, or *IOS*. The IOS features a command-line interface (CLI), which is accessible using a serial cable or a LAN Telnet connection.

We shall use the IOS command-line interface in four modes of operation, which are described in the table 8.3. As shown in the table, you can identify the current mode of operation according to the CLI prompt. The *user EXEC* mode offers limited information about the switch. The *privileged EXEC* mode allows us to access detailed information. The *global configuration* mode enables us to configure the general aspects of the switch, whereas we can use the *interface*

Command Mode	CLI Prompt	Access
User EXEC	`Switch>`	By default, when connecting to the switch for the first time, you are in this mode.
Privileged EXEC	`Switch#`	From the User EXEC mode, enter the `enable` command.
Global Configuration	`Switch(config)#`	From the Privileged EXEC mode, enter the `configure terminal` command.
Interface Configuration	`Switch(config-if)#`	From the Global Configuration mode, enter the `interface <if-name>`, where `if-name` is the name of the interface that we want to configure, such as `FastEthernet0/4` or `Fa0/4`.

Table 8.3: *Command modes of the Cisco IOS command-line interface*

configuration mode to configure a specific interface. The commands available in each of the modes are different. Make sure you are in the right mode before issuing a command. After entering a specific mode, it is possible to leave to the previous one using the command:

```
exit
```

Use a Telnet client to connect to the switch and observe which is the initial mode. You can use the command:

```
?
```

to obtain information about the possible commands in a given mode. Additionally, you can also follow a partial command by ? to obtain more information about how to use the command and the required parameters. For example, the command:

```
ip address ?
```

would give you information about the parameters you could use after address.

Enter the *privileged EXEC* mode and use the command:

```
Switch# show running-config
```

to see the current configuration of the switch.

Questions (3 × 3 %)
How many VLANs can you observe? Note that this is not necessarily the number of VLANs in the switch.
How many Fast Ethernet interfaces are available?
What is the VLAN1 administrative address?

There exists a *default* VLAN which has the number 1. Use the command:

```
Switch# show vlan
```

or

```
Switch# show vlan id <id>
```

to collect more information.

Questions (2 × 3 %)
What is the status of VLAN1?
How many VLANs are there in the switch? For each of the VLANs identify the ID, the name, the status, the assigned ports and the type. Include this information in the report.

Enter the *global configuration* mode and try to delete the default VLAN.

```
Switch(config)# no vlan 1
```

Question (3 %)
What happens?

Use the ? command to find which commands can be used in this mode. Create a new VLAN with the command:

```
Switch(config)# vlan <id>
```

The type of the VLAN is Ethernet and the `id` must be set according to the sketch you find on the blackboard/whiteboard. Include the exact command that you used and the reply message of the router in your report.

Verify the new configuration using the following command:

```
Switch# show vlan
```

in the privileged EXEC mode.

Question (3 %)

What is the default name of the new VLAN?

Delete the VLAN that you have just created using the command:

```
Switch(config)# no vlan <id>
```

and verify that it has been deleted and create it again.

Include in your report the sequence of commands that you used and the output of the switch after each command. You can use the command:

```
Switch# show vlan brief
```

In the *global configuration* mode, use the command:

```
Switch(config)# vlan <id>
```

to configure the VLAN that you have created. In the *VLAN configuration* mode use the `name` command to change the name of the VLAN.

```
Switch(config-vlan)# name <vlan-name>
```

Name your VLAN `vlanXX-GroupX-switchX`, and verify the changes. Include in your report the exact commands that you used and the output of the switch.

Question (3 %)

Which other parameters can be changed in the VLAN configuration mode?

In the *privileged EXEC* mode, take a look at the running configuration and compare it with the start-up configuration.

Question (3 %)

Are they equal?

Find which are the commands that are needed to show the running configurations, and then to copy the running configuration to the start-up configuration. You will need this command when you make changes to the configuration that you want to save.

Tasks (3 %)

Add these commands to your report.

	Same switch	Different switch
Same VLAN	Yes/No	Yes/No
Different VLAN	Yes/No	Yes/No

Table 8.4: *Connectivity tests*

8.4 Static Assignment of a VLAN

After creating one or more VLANs, during the next step we assign ports to the VLANs. The simplest assignment is the *static* assignment. First, enter the *global configuration* mode. Find out which are the ports that you want to modify (for example, 0/1, 0/2, etc.).

Important

Modify only the configuration of the ports that are assigned to the other two computers from your group. Make sure that you do not change the port that you are using for the Telnet connection.

To make the changes, you first have to go into to *interface configuration* mode. Here, check the options of the `switchport` command and use the switch user manual if you require extra information. After making the changes, return to the *privileged* mode. Verify the changes that you have made comparing the running configuration to the start-up configuration. Save your changes.

Tasks (6 %)

Add to your report the output of the commands showing that you successfully assigned the ports to your VLAN.

Use the `ping` command to test the connectivity between the two auxiliary computers. Try the connectivity between the configuration computer (the one that you use to connect to the switch CLI) to the auxiliary computers. Finally, try the connectivity between the computers of your group and computers of other groups in your class.

Questions and Tasks (3 × 3 %)

Which devices are reached if you use a broadcast packet?

How can a packet travel from one VLAN to a different VLAN?

Explain the results and the conclusions of the experiments, and complete the table 8.4.

8.5 Trunk Ports

A trunk port can carry traffic of different VLANs between two switches. You will find which are the trunking ports on the blackboard/whiteboard. In the *privileged EXEC* mode use the command:

```
Switch# show interfaces <interface> switchport
```

Task (7 %)

Write down the following parameters:

- Administrative mode
- Operational mode
- Administrative trunking encapsulation
- Trunking native mode
- Trunking VLAN enabled

Use the command:

```
Switch# show vlan
```

to check the status of the ports.

Question (3 %)

How can you find the trunk ports?

8.6 VLAN Trunk Port Assigment

By default, a trunk port carries traffic of all VLANs. However, it is possible to configure which VLANs are allowed in a given trunk port. To accomplish this, from the *privileged EXEC* mode, check which are the VLANs in the trunk port of your switch.

Question (3 %)

What command do you use to find the trunk ports of your switch?

In the *global configuration* mode, enter into the configuration of the trunk port. Now we are going to configure the trunk port to allow the traffic of our VLAN. Check the options of the command:

```
Switch(config-if)# switchport trunk allowed vlan { remove | add } <vlan-list>
```

The parameter `vlan-list` is a list of VLAN identifiers (or names) separated by a hyphen (`-`) when specifying a VLAN range, or a comma (`,`) when specifying a set of VLANs.

Question (6 %)

What commands do you use to configure a trunk port?

Exit the configuration mode and return to the *privileged EXEC* mode. Use the commands:

```
Switch# show interface interface-id status
```

or

```
Switch# show interface status
```

to see the configuration of one or all the interfaces.

Question (3 %)

What are the results?

Student Group	Computer	New IP Address
Group X	Computer using VLAN 10	192.168.20.1X/24

Table 8.5: *The new IP address of one of the computers.*

Try also the command:

```
Switch# show interfaces trunk
```

Task (3 %)
Include the output of the previous command to your report.

Verify whether the following connections are possible and explain why.

Questions and Tasks (4 × 3 %)
Can you ping a computer of the same VLAN, connected to a different switch? Include the output of the ping command.
Compare the results that you obtain now with the results obtained in the static assignment of VLANs. Fill in the connectivity table 8.4 again.
Are there any differences from the previous table? Explain.

Change the IP address of *one* of your auxiliary computers to an address belonging to the range of the other VLAN, as shown in the table 8.5. Perform the connectivity tests again.

Question (3 %)
What changes? Why?

Task (3 %)
Draw the network topology, both from the physical point of view and the logical point of view.

8.7 Changing the Native VLAN (Optional)

For security reasons, it is recommended to change the native VLAN of the switches (for example, to 666) and leave no ports assigned to that VLAN, except for administration.

8.8 Speed and Duplexing (Optional)

Change the speed of the port and the duplexing type and perform tests using `iperf`.

8.9 Administrative Shutdown of an Interface (Optional)

Try to administratively disable access ports and trunking ports and describe the results.

Chapter 9

Spanning Tree Protocol (STP)

9.1 Home Preparation

Important
For this practical exercise, you have to submit a report the answers to the questions below. When submitting the answers to the questions, be brief but precise. If you include screenshots, indicate on the screenshot what is the answer.

The user manual for the switch is available here:
http://www.jaumebarcelo.info/teaching/lxs/stp/manual_spantree.pdf

9.2 Introduction

In this assignment you will configure the Spanning Tree Protocol (STP). This protocol is used in Ethernet networks to establish which are the active link and therefore which is the path that data packets will follow. The switches that you will use are the same as the ones in the previous assignment. Have your VLAN report handy just in case you need to consult it and to remember which are the basic commands to interact with the switch.

9.3 Theoretical Construction of the Tree

The switches are connected as illustrated in the figure 9.1.

Questions and Tasks
If the priority is `32768` (`0x8000`), what is the `Bridge ID` of each switch? (5 %)
Which is the root switch? (5 %)
Compute which is the spanning tree and draw it. (10 %)
Fill in the table 9.1, indicating for each switch the role and state of each trunk port. (10 %)

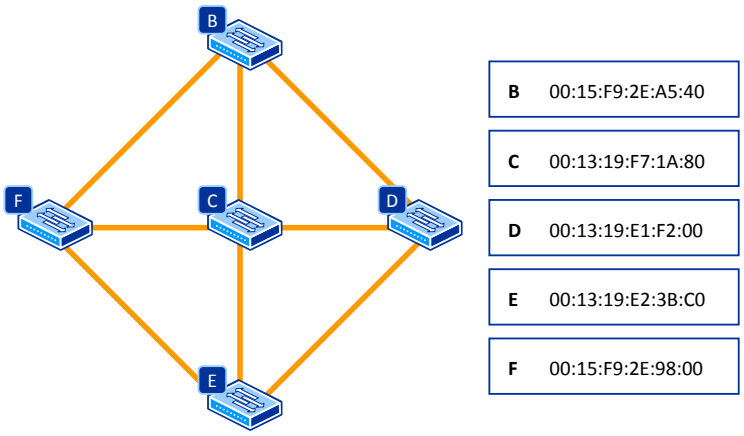

Figure 9.1: *The network topology used for the STP practical exercise.*

Switch name	MAC	Bridge ID	Port	Role	State
Switch B	00:15:F9:2E:A5:40	?	?	?	?
Switch C	00:13:19:F7:1A:80	?	?	?	?
Switch D	00:13:19:E1:F2:00	?	?	?	?
Switch E	00:13:19:E2:3B:C0	?	?	?	?
Switch F	00:15:F9:2E:98:00	?	?	?	?

Table 9.1: *The spanning tree.*

9.4 Practical Verification

Now you will verify that the STP constructed by the switches is in fact the one you computed in the previous section. Use the VLAN 1 to connect to the five switches (B, C, D, E, F). It is recommended to open five simultaneous Telnet connections, one for each of the switch.

Each group will work in a different VLAN. The teacher will assign a VLAN to each group. Make sure that your VLAN is included in all the trunk ports. Each group will have a different STP, as the network creates a tree for each VLAN.

In each of the switches, enter the *privileged EXEC* mode and use the command:

```
Switch# show spanning-tree vlan <id>
```

Observe all the fields and make sure you understand them.

Questions and Tasks
What is the `Bridge ID` of each switch? Indicate the MAC and the priority. (5 %)
For the `Bridge ID` priority of each switch, what is the base priority value set by the switch administrator? (5 %)
Compute which is the spanning tree and draw it. (5 %)
Fill in the table 9.1, indicating for each switch the role and state of each trunk port. Are the theoretical and practical results identical? (5 %)

9.5 Changing the STP Configuration

Now that you are familiar with the STP parameters, you will make some changes that will result in the computation of a new tree. In the *global configuration* mode use the command:

```
Switch(config)# spanning-tree vlan <id>
```

or, alternatively, you may use:

```
Switch(config)# interface vlan <id>
Switch(config)# spanning-tree
```

to see which parameters are susceptible to be configured. Use the question mark `?` to see all the available parameters and make sure you understand them.

The exercise that we propose is to change the priority of one of the switches different from the root switch. The default behavior is that the switch with the lowest MAC address is selected as a root. The reason is that, in the default configuration, the priority of all the switches is `32768` (`0x8000`). By changing the priority of one of the switches to a lower value, we can force that that particular switch becomes the root.

Change the priority for the root switch and observe the new configuration of the tree.

Questions and Tasks
Compute which is the new spanning tree and draw it. You must indicate the new priority you assigned to the previous root switch. (10 %)
Fill in the table 9.1, indicating for each switch the role and state of each trunk port. (10 %)

9.6 Link Failure

Important
For this assignment you must wait until all the groups have finished the previous one. If you reach this exercise before the other groups, move on to the next exercise while you wait for all the groups to be ready for the link failure.

Now we will disconnect one of the links to simulate a link failure. Compute in advance your new spanning tree after the link failure. Ask your teacher which is the cable that will be disconnected. After the disconnection, check which is the new configuration and compare it with the one that you have predicted.

Questions and Tasks
Compute which is the new spanning tree and draw it. You must indicate the link that failed. (10 %)
Fill in the table 9.1, indicating for each switch the role and state of each trunk port. (10 %)

9.7 BPDUs

Use the computer connected to the VLAN 1 (the computer used for the administration of the switch) and capture the traffic for several seconds using *Wireshark*. Observed the received STP frames and identify the different fields in the packet.

Questions and Tasks

Include in your report one received STP BPDU, and indicate what the information from the main fields. Tip: Use the lecture notes to identify the relevant fields. (10 %)

Chapter 10

Routing

10.1 Home Preparation

Important

For this practical exercise, you have to submit a report the answers to the questions below. When submitting the answers to the questions, be brief but precise. If you include screenshots, indicate on the screenshot what is the answer.

RIP and OSPF are two of the most widely used routing protocols. Find information about these two protocols and compare them. Describe what is the format of a routing table and explain how each of the protocols work.

Read the following quick guide:

www.jaumebarcelo.info/teaching/lxs/routing/GUIA_RAPIDA_CISCO_2010.pdf

Then, download the router user manuals:

www.jaumebarcelo.info/teaching/lxs/routing/manuals_routers.rar

10.2 First Session

Important

Each group must select a computer that has a console serial connection.

Start your computer in Windows.

Before disconnecting the computer from the Internet, download the TFTP server from the web site http://tftpd32.jounin.net/, and save it on one of the computers that you will use to connect to the router.

In this first session each group will work with a router. The goals of this session are:

- Getting familiar with the configuration method.
- Configuring the Ethernet interfaces.

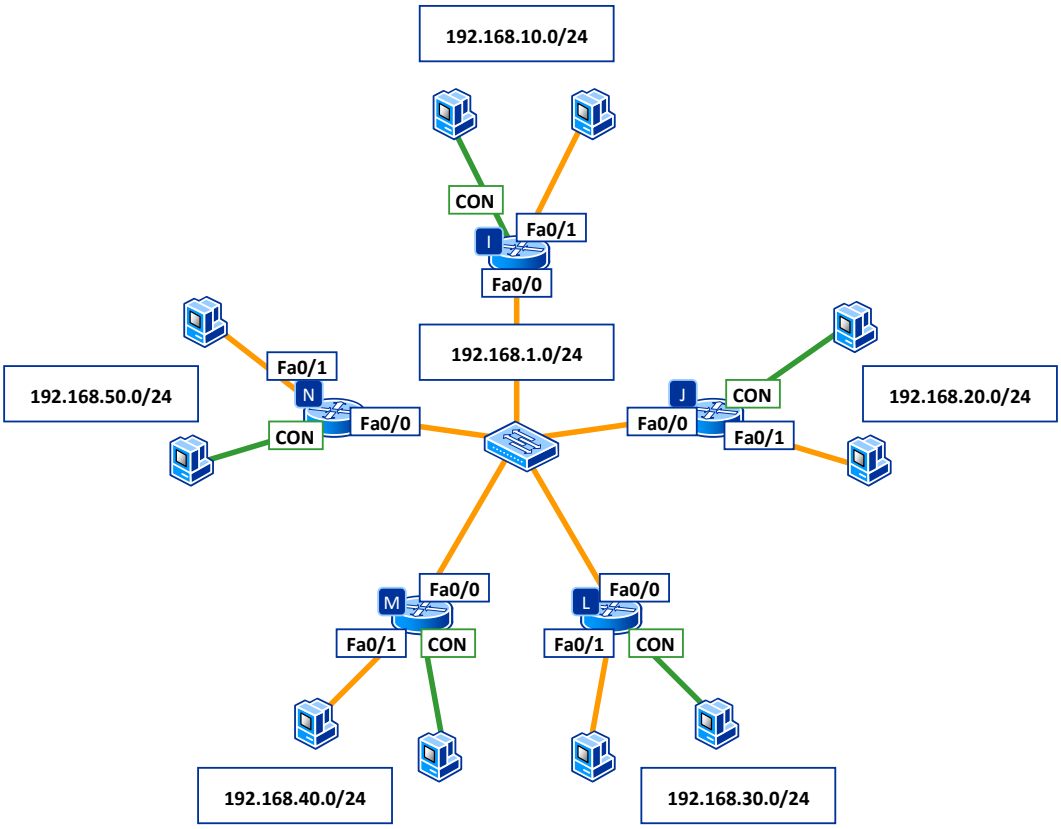

Figure 10.1: *The network topology used for the Ethernet routing exercise.*

- Observe the RIP protocol in action.
- Save the configuration in an external TFTP server.

The routers are connected to each other using the Ethernet interfaces and forming the topology from the figure 10.1. Use the console connection to connect to the routers (use *PuTTY* to open a serial connection at 9600 bps). The COM port number (e.g. COM1, COM2, etc.) depends on your computer configuration[1]. The escape keystroke to exit the `ping` command in a router is Ctrl-Alt-6.

10.2.1 Checking the Router Status

Use the console to connect to your router and try the following commands. Prepare a summary of what you can see with each command.

```
show history
show protocols
show interfaces
show ip route
```

Questions (4 × 3 %)

For each of the previous commands, what does the output represent?

[1] You can see the name of the local serial ports in the *Device Manager* snap-in. To open the snap-in, click on Start >Run..., type `devmgmt.msc` and click OK. The serial ports are listed under the *Ports* branch.

10.2.2 Create a Running and Startup Configuration

Enter the privileged EXEC mode with the command:

```
Router> enable
```

and password `cisco`, and the the global configuration mode

```
Router# configure terminal
```

Tasks (4 × 3 %)

Find and include to your report the commands to:

- show and change the router name;
- debugging mode configuration;
- send pings from the router, and;
- activate fair queueing on the ethernet interfaces (e.g. FastEthernet0/0).

Use the following commands to show and save the current configuration to the startup configuration from the privileged mode.

```
Router# show running-config
Router# copy running-config startup-config
```

10.2.3 IP Addresses Configuration

Go to your physical router equipment and check which interfaces are visible. Use the following command to see what interfaces are available in the router.

```
Router# show interfaces
```

Tasks (5 %)

Include in your report a table with the following information for each interface:

- the interface name;
- the interface MTU;
- the interface bandwidth, and;
- the encapsulation protocol.

Enter in the configuration mode of the Ethernet interface with the command:

```
Router(config)# interface <interface name>
```

Then, set the IP address to `192.168.X0.1`, where `X` is the number of your group. Use a /24 network mask. Use the IP address `192.168.X0.2` for the Ethernet interface of your computer.

Question (5 %)

What is the command to configure the IP address on the router interface? Indicate the command mode in which you must execute this command.

Use the command:

```
Router# show interfaces
```

to verify the IP address assignment, and enable the interface with the command:

```
Router(config-if)# no shutdown
```

Task (5 %)

Include in your report the relevant output of at least one command showing that you successfully configured the IP address on the Ethernet interface.

Verify the line status and the interface status using the command:

```
Router# show protocols
```

Use the commands:

```
Router# show cdp neighbors
```

and:

```
Router# show cdp neighbors detail
```

to see the neighboring Cisco devices.

Question and Tasks (5 %)

What are the devices displayed by the `show cdp neighbors` command? Write down the information received from the different interfaces.

- the neighbor identifier;
- the IP address, and;
- the port.

Use the `ping` command to test the connectivity to at least one other router in the lab.

Task (5 %)

Include in your report the output of the `ping` command, indicating the round-trip times.

From your computer, use the PuTTY in Telnet mode to connect to your router.

Questions (5 × 1 %)

Is it possible to remotely configure a router using Telnet?

Is login and password required?

Does a console user notice that there is an ongoing telnet connection?

Use telnet to change a parameter of the router (such as the router name) and verify the changes both using the console and the telnet connection. What happens?

Do any messages appear on the console when changes are done over Telnet? What information is included in these messages?

Logout the Telnet session to the Cisco router.

10.2.4 IP Routing Configuration

In this exercise, we shall enable the RIP protocol and check the status of the routing table as well as the RIP transactions of each router.

Check whether IP routing is enabled using the command:

```
Router# show protocols
```

Question (5 %)

What is the status of IP routing?

Enter the global configuration mode and enter the submenu `router`.

Question (5 %)

What is the purpose of this submenu?

Use the `?` command to list available routing protocols and write down the results. Enter into the configuration of RIP.

```
Router(config)# router rip
```

Use the command:

```
Router(config-router)# network <network>
```

to associate your network to the RIP routing process. Assume that we are working with C class IP addresses. Therefore, the last byte of the network address must be 0. Verify that the RIP protocol is now enabled and that your network has been recognized by the router using the command:

```
Router# show ip protocol
```

Task (5 %)

Include in your report the output of the previous command showing that the RIP protocol has been enabled.

Observe the relevant parameters and answer the following questions:

Questions (3×2 %)

What timers do you identify for the RIP protocol?

What are their values?

What happens if we change the values?

Verify the status of the routing table with the command:

```
Router# show ip route
```

Task and Questions (3×2 %)

Include in your report the routing table of your router, after the RIP protocol has been enabled on at least one other router in the lab.

What is the meaning of each of the fields in the table?

How do you identify the networks advertised using the RIP protocol?

Important

For this assignment you must work together with another group. If there is no other group ready, skip this exercise and come back to it when another group reaches this point.

Add a static route to the other group's network. Use the following command from the configuration mode.

```
Router(config)# ip route
```

Task (5 %)

Include in your report the command you used to setup a static route.

Use the `traceroute` command from your computer, choosing as destination the computer of another group.

Question (5 %)

Include the output of the traceroute command, indicating the network interfaces traversed by the traceroute ICMP or UDP packet?

Use the command:

```
Router# debug ip rip
```

to show the RIP messages that are sent and received by the router.

Questions (2 × 2 %)

What are the source and destination of these packets?

What information do we obtain?

10.2.5 Saving the Router Configuration in a TFTP Server

A convenient way to store a router's configuration is using TFTP. We need to install the TFTP server in a computer with connectivity (layer 3 connectivity) to the router. Install the server and configure in which folder you want to save the router's configuration.

In the router, execute the command:

```
Router# copy running-config tftp
```

and follow the instructions to enter the TFT server address (this is one of your computers) and the filename that you want to use. In the computer, open the configuration file using a text editor.

Question (5 %)

What is the format of the configuration file saved on your computer? How is the content of this file compared to the configuration file viewed in the router console?

To copy the configuration in the TFTP server to the router, there are two different options. Use either the command:

```
Router# copy tftp running-config
```

on the server or simply copy and paste on the configuration terminal.

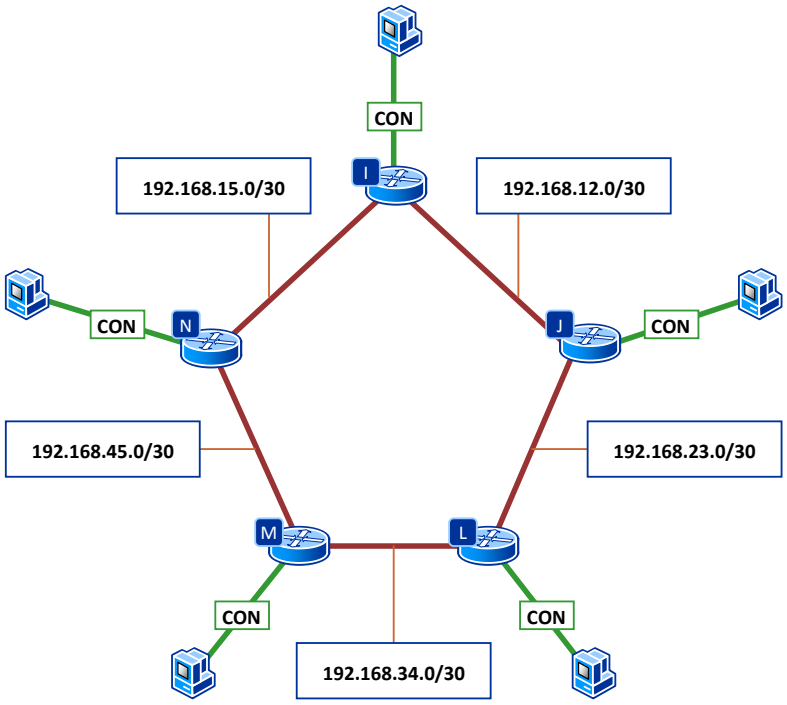

Figure 10.2: *The network topology used for the WAN routing exercise.*

10.3 Router Interconnection

In this session, we shall use the WAN (serial) interfaces of the routers. The figure 10.2 illustrates the topology of the network. In the previous session we used the Ethernet interfaces to connect the routers, and in this session we will use the serial interfaces.

10.3.1 Shutdown the Ethernet Interfaces

Make sure that there is no cable connected to the Ethernet interface, and that there is a cable connecting the serial interfaces. Delete the IP address of the Ethernet interface:

```
Router(config-if)# no ip address
```

and administratively shutdown the interface:

```
Router(config-if)# shutdown
```

Verify that the changes have been applied using:

```
Router# show running-config
```

Task (5 %)

Include in your report the final configuration of the Ethernet interface.

10.3.2 Configuration of the WAN Serial Interface

The serial interfaces are interconnected by cables that, in the middle, have male/female connector. The router in the female connector side sets the communication rate. You can find which is the female router issuing the command:

```
Router# show controller
```

The DTE interface uses the male connector, and the DCE interface uses the female connector. Alternatively, you may also look at the number on the cable, where 1428 is male and 1429 is female.

Question? (5 %)

What type of connector do you use for each of the serial interface?

From the privileged mode of your router, enter the global configuration mode. Enter into the configuration of the WAN serial interface and configure the IP.

To choose the IP, use the following algorithm. Assume the your group id is `X` and your neighbor's group ID is `Y`. If `X` <`Y`, then your IP is `192.168.XY.1`. Otherwise, it is `192.168.YX.2`. Use a /30 network mask.

Task (5 %)

Include in your report the commands you used to setup the IP addresses on each serial interface.

On the DCE serial interface, you must setup the interface clock rate. Using this practical exercise we shall use a clock rate of 128 kbps. Use the command:

```
Router(config-if)# clock rate <bps>
```

or the closest available rate.

Verify the previous configuration is correct and enable the serial interfaces using the command:

```
Router(config-if)# no shutdown
```

Task (10 %)

Include in your report the final configuration of the serial interfaces.

Wait for your neighbors to complete their configuration, and then use the command:

```
Router# show protocols
```

to verify the state of the line.

Task (5 %)

Include in your report the state of each serial interface.

Now we will gather information about neighboring devices using the command:

```
Router# show cdp neighbors
```

or

```
Router# show cdp neighbors detail
```

Task (10 %)

Elaborate a table indicating, for each neighbor, the following information:

- the neighbor identifier;
- the neighbor IP address, and;
- the port.

Enable routing using the following commands:

```
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network <network>
```

and look at the routing tables using the command

```
Router# show ip route
```

Tasks (2 × 10 %)

Include in your report the current routing table.

Compare the routing table to the one obtained in the previous session and highlight the differences.

Use the `ping` tool to measure the connectivity to the other routers in the network.

Tasks (2 × 5 %)

Indicate which routers are reachable and which are not. Explain why by using the current routing table.

Are there differences in the round-trip-time compared to the measures taken in the previous session? Why?

10.3.3 Network Topology

Compare the current network topology to one of the previous session. Answer in a few brief sentences to the following questions.

Questions (3 × 10 %)

What are the differences between the two networks? Enumerate at least three (3).

What are the advantages of the current topology over the previous one?

What are the disadvantages of the current topology over the previous one?

10.4 Configuration of an L2-L3 Network

This third session extends the previous one by including switches to the network topology, as shown in the figure 10.3. The topology consists of a ring of routers connected in a ring using the serial interfaces. Each router is connected using the Ethernet interface to a local area network with two or more computers. The devices used in this assignment are:

- computers;

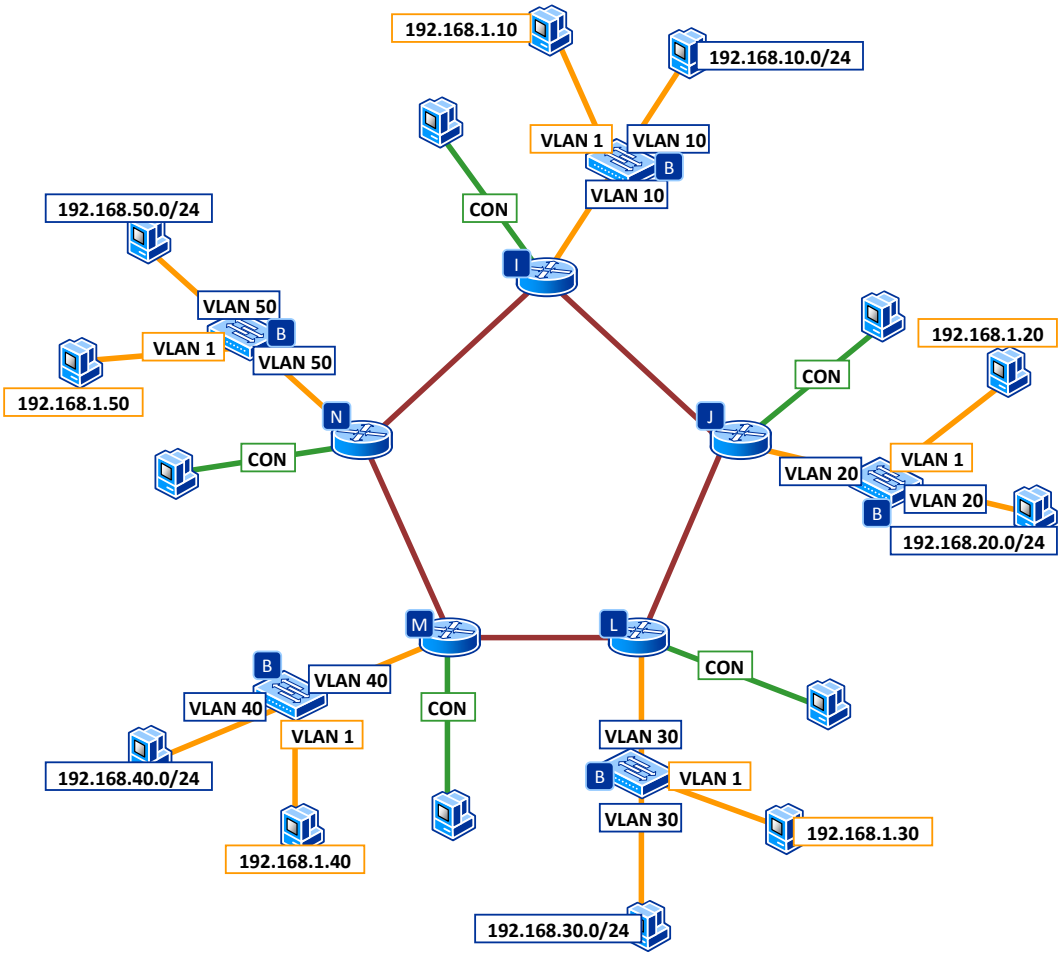

Figure 10.3: *The network topology used for the L2-L3 network.*

- up to six Cisco routers with an ethernet interface and two serial interfaces;
- up to three Cisco switches, and;
- direct and cross-over RJ-45 cables.

Each group has to configure its router and its VLAN. It is assumed that the previous session has been successfully completed and the connectivity tests were satisfactory.

During this practical exercise, each group shall fill in a form indicating the desired configuration for the computers and network equipments involved.

Task (10 %)

Download the form for your part of the network topology from the following address:

`http://alex.bikfalvi.com/teaching/upf/2014/networks_and_services/lab/routing/FormRouting.pdf`

Fill in the configuration of all computers and network devices.

10.4.1 VLAN Configuration

We connect using Telnet to our switch and enter the privileged mode. Create a VLAN with a number equal to ten times your group number (e.g. VLAN 20 for group 2). Assign a port connected to the router and one or two other ports connected to computers. Remember to keep the port of the computer you are using for managing the switch in VLAN 1.

Use an IP equal to `192.168.1.X0` where `X` is the number of your group, for the computer in VLAN 1. Use an IP `192.168.X0.X` for the other VLAN. `Y` is 1 for the router and 2 for the computer. You can use `X` equal to 3 if you have another computer.

Tasks (3 × 15 %)

Include in your the commands you used to setup the VLAN configuration.

Include in your report the VLAN configuration showing that you successfully assigned your VLAN on the required interfaces.

Include in your report the configuration of the interfaces you used.

Test the connectivity between your different computers and with computers of other groups. Write down when a `ping` command is successful and when it is not successful, and provide an explanation.

10.4.2 Configuring the Router LAN Interface

In the router console enter the privileged EXEC mode and use the command:

```
Router# show interfaces
```

to see the interfaces which are available in the router. We enter the global configuration mode and in in the configuration of the LAN (Ethernet) interface. We configure the IP for this interface. Then we enable the interface with the command:

```
Router(config-if)# no shutdown
```

and check the link status LED. We can also check the status of the line and the interface using the command:

```
Router# show protocols
```

Then we enable the routing. From the global configuration menu we enter the router menu and we use the command:

```
Router(config-router)# network 192.168.<vlan>.0
```

to associate our network to the routing process. We will assume that we are using class C networks. Then we use the command:

```
Router# show routes
```

to see the routing tables.

Tasks ($2 \times 15\,\%$)

Include in your the commands you used to setup the configuration of the router's Ethernet interface and to enable IP routing using RIP.

Include in your report the final state of your routing table. Indicate which are the networks that are reachable from your router, and how these networks were discovered.

10.4.3 Connectivity Test

We add our router's IP as as the default gateway for the computers connected to the router. We perform ping tests from the router to the other devices of the network. Then, we repeat the same tests from a computer. If we are on a Linux box, we may also try the `tracepath` and `mtr` commands.

Tasks ($3 \times 7.5\,\%$)

Include in your report a table with the results of the connectivity test performed from your router, which must include following information:

- the destination IP address;
- the packet loss, and;
- the average delay.

The connectivity test must involve at least one other router and one other computer.

Include in your report a similar table with the results of the connectivity test performed from your computer.

Chapter 11

Firewall

The goals of this assignment are the following.

- Familiarizing ourselves with firewalls.
- Correctly configuring the different options.
- Configuring a local area network, establishing different security polices using filtering and traffic monitoring.
- Solve a case study about connecting a Small/Medium Enterprise (SME) network to the Internet using a firewall.

11.1 Home Preparation

The Cisco firewall can be configured using a Java program which is called *Adaptive Security Device Manager* (ASDM). This tool makes it possible to interact with the firewall using a graphical user interface (GUI) on a computer with the Windows operating system.

Read more from the following document: www.jaumebarcelo.info/teaching/lxs/ipsec/ASA_Getting_Started.pdf Read also all the assignment and prepare a solution for the *case study*.

You can download a copy of the Cisco ASDM software from the following link. https://www.dropbox.com/s/5yjqflzvgrlere0/asa.zip

In the beginning, we can familiarize ourselves with the Adaptive Security Device Manager (ASDM) software using a demo version. The software requires the Java Runtime Environment (JRE) version 1.6.18. After installing and launching the program, select the Run in Demo Mode checkbox and choose the desired demo version. The version we use during this practice is 5.2.

11.2 Configuring the working place

For this practical exercise, each group needs 3 computers and a Cisco ASA 5505 firewall. Connect one of the computers to switch B via the patch panel. Before disconnecting this computer from the Internet, download an FTP server such as *Filezilla*. Connect the other two computers to the two internal ports of the firewall (ports 2 and 3).

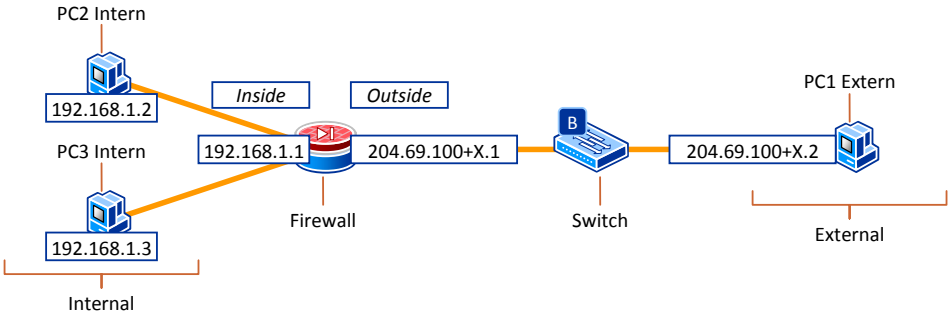

Figure 11.1: *The network topology for the firewall lab assignment.*

Important

Write down the UPF number of your firewall so you can identify it in the next session.

Connect the firewall to the switch B via the patch panel. Configure the IP address on the external interface (*outside*) of the firewall according to the figure 11.1, where X is the number of your group. Configure the default gateway of the three computers with the IP address of the corresponding firewall interface, internal (*inside*) for the internal computers and external (*outside*) for the external computers.

We shall use the FTP to verify that our network configuration works. Identify the transport layer protocol and the port number for FTP.

11.3 Adaptive Security Device Manager (ASDM)

We will find a shortcut to the *ASDM* application on the desktop. In the case the ASDM is not installed on your computer, open Internet Explorer, disable the proxy and navigate to `https://192.186.1.1`, where the default IP address of the firewall is 192.168.1.1. The default username and password are blank. From the firewall's web interface, use the first button to download and install the ASDM on your computer. Once you open the ASDM, use the same IP address, username and password to connect to the firewall.

The CISCO ASA firewalls assign a *security level* to the interfaces. A security level of 100 means the interface is 100% trusted. A security level of 0 means that the interface is not trusted at all. We shall check the interfaces available and their security level. Discuss the appropriateness of this configuration.

We try to ping between the two computers connected to the internal interfaces.

Question

Does it work? Why?

11.4 Default Configuration of the ASA 5505

The Cisco ASA use the same OS that the other devices used in the previous assignments, the Cisco IOS. Open the Options >Preferences menu and check the Preview commands before sending them to the device option. This will show us the equivalent commands that would be used on the console to change the configuration.

Explain which is the default configuration of the firewall. Observe and explain the different aspects that can be configured using the icons on the left hand side of the screen.

Questions
What is the default configuration of Ethernet 0/0 (outside)?
Why do you thing that the router ships with this configuration?

Now, we will change the IP address of the Ethernet 0/0 (*outside*) interface to 204.69.100+X.1. Remember that the X is the group number, and use a /24 network mask. Now we connect the external computer (via switch B) to the *outside* interface. We configure the IP of the external computer to an address of the outside range and we set the firewall's outside address as the computer's default gateway.

Questions
Can you ping from the outside PC to an inside PC? Why?
What is the difference compared to the previous case?

Look at the Syslog from the Home screen to answer this questions.

11.5 Firewall

An alternative configuration option is Telnet. We can enable the Telnet options from the ASDM configuration page using Properties >Device Access >Telnet. We have to make sure that we have applied the changes. Now we connect to the device using a Telnet client and `cisco` (small letters) as a password.

We try the

```
# who
```

command to see who is connected to the firewall.

```
# show run
```

to see the running configuration. Find information about Telnet and DHCP and explain it. We also try the commands

```
# show interface
```

and

```
# show traffic
```

and explain the information that they provide.

Discuss the security implications of connecting using Telnet of the console.

11.6 The Hosts/Networks Table

In the Network Objects/Groups tab (from the Configuration >Global Objects page) we can view, edit, add and delete hosts and networks lists defined for every interface. The hosts and networks are organized according to the interface they are connected to (inside/outside). It is recommended to name all the hosts we are managing.

We add the two internal computers by selecting Add >Network Object.... The network mask is 255.255.255.255, as it is a single host. Add also a corresponding object for the external computer. We apply to save the changes.

11.7 Access Rules

The access rules make it possible to establish security policies as a list of rules. The tables to specify how a computer interacts with another by allowing and denying specific services and protocols. We try to connect from the inside computer to the outside computer and explain the behavior and the default Access Rules (from the Configuration >Security Polivy page) table for the inside interface.

The rules are examined sequentially until one of the applies. If the first rule applies, the second is not checked. If the first rule does not apply, then the second is checked. The process is repeated until one of the rules applies.

Question
The last rule is any to any deny. Why?

The first rule allows traffic from any IP source to any IP destination if the destination interface has a lower security level. If this rule does not apply, the second rule is examined. The second rule always applies and discards the packet.

We shall observe and explain the rules for the traffic arriving to the external interfaces. To understand the rules, we will pay attention to the graphical diagrams offered by the software.‘

We shall install and configure the FTP server to the external computer. Remember that it is needed to add a folder.

Question
Is it possible to access the FTP server from the internal computers?

Use the rules to deny the access to the FTP server to one of the internal computers and allow access to the other. Observe the log messages to verify that access is being denied. Each time that you change the configuration and try to access to the ftp server, clean the browser cache.

11.8 Translation Rules

The ASA 5505 supports both network address translation (NAT) which is a one-to-one address translation (one inside to one outside) and port address translation (PAT) which is a many-to-one address translation. Look at the default configuration for the translation rules.

Questions
How does this configuration affect outgoing traffic?
What is the IP address used after the packets traverse the firewall?

11.9 Monitoring

We can use the ASDM for network monitoring. It allows to select the message supervising level. Check the Telnet connections and connected users using the options of the menu on the left. There is also a tool to generate graphs such as traffic, memory and CPU. Look at some of the graphs and enumerate them.

11.10 Case Study

An enterprise has a C class network 204.69.100+X.0 and wants securely connect their internal network to an external network. The address of the outside firewall interface is 204.69.100+X.1.

In the internal network there is an FTP server with address 192.168.1.4 that needs to be accessed from the outside network using the address 204.69.100+X.4.

The other requirements are that internal users must be able to ping external devices, but not the other way around.

We shall configure the firewall to satisfy the above requirements. Explain the changes that we have made and the tests performed to verify the correctness of the configuration.

Chapter 12

Final Project

In this project we shall configure a network combining the different technologies that we have learned during this course. In particular, we shall extend the topology in the routing assignment with wireless connectivity (WLAN) and security (firewall) and traffic monitoring (Wireshark).

12.1 Topology

The topology that we will construct is presented in the figure 12.1. Similar to the routing assignments, each group will configure a part of the topology. In this assignment, each group will take care of a router, a firewall, a switch, an access point and the necessary computers. This topology interconnects secured networks (behind a firewall) with another network that offers access to the Internet. Each secured network needs at least one PC with an FTP server.

Important
You should ask for the same firewall that you used during the firewall assignment.
Write down the UPF (or serial) number of your firewall and access point so you can identify them in the next session.

12.2 Equipment and Addresses

The assignment of equipment and addresses to the groups is detailed in the table 12.1. The switches are shared and the table specifies the ports for each group. The IP addresses for WLAN devices, Ethernet devices, the firewall interior interface and the public addresses are also included.

Within each private subnetwork, we shall reserve the 172.29.X0.0/24 range for the Ethernet devices, and we shall use the 172.29.X1.0/24 range for the WLAN devices. We shall assign *static* IP addresses to the computers using wired Ethernet connections, whereas the WLAN computers shall receive their IP address using *DHCP*.

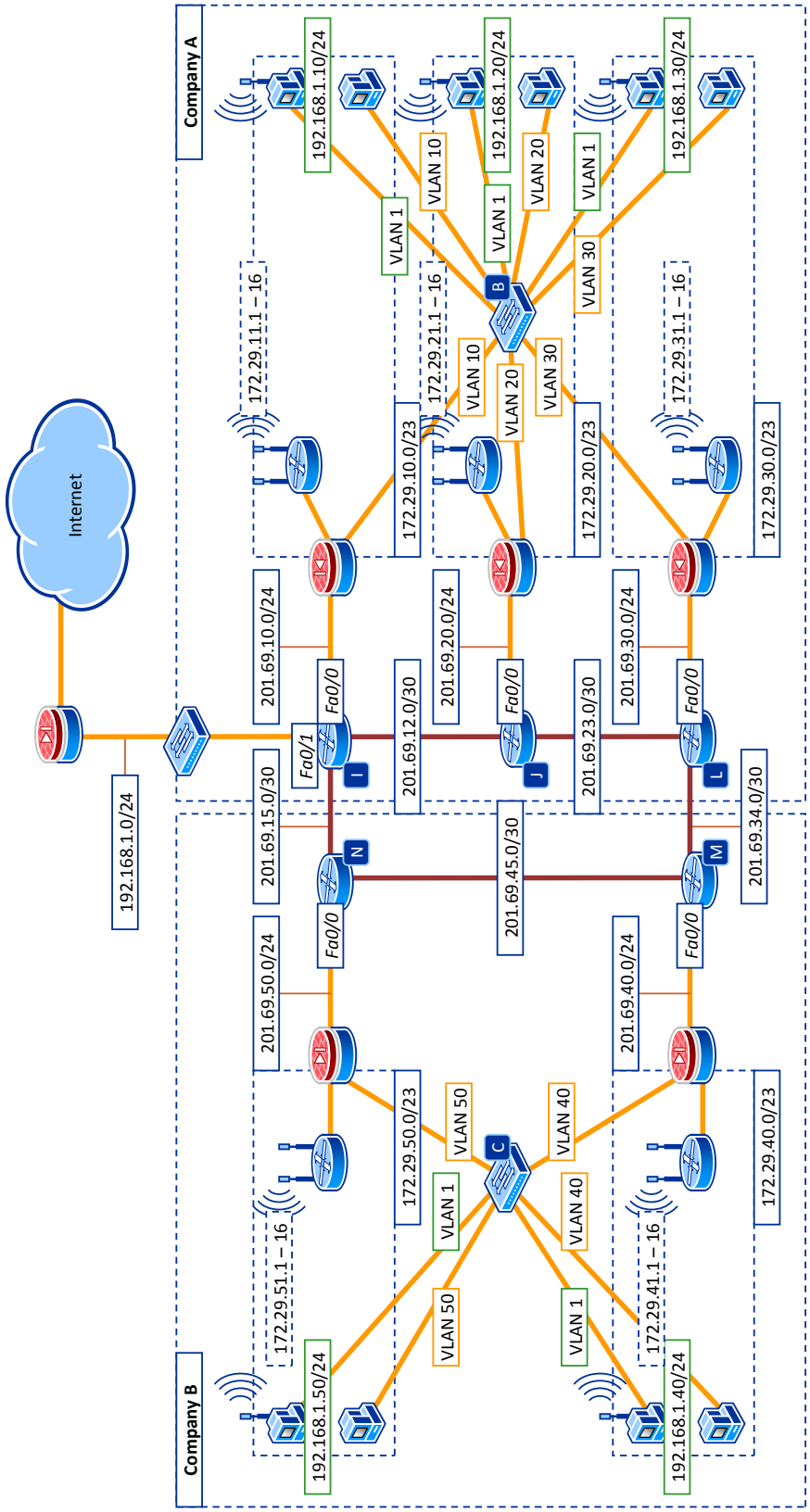

Figure 12.1: *Topology of the final assignment*

Group	Router	Switch	Ports	Public range	Private range
1	I	B	1-8	201.69.10.0/24	172.29.10.0/23
2	J	B	9-16	201.69.20.0/24	172.29.20.0/23
3	L	B	17-24	201.69.30.0/24	172.29.30.0/23
4	M	C	1-8	201.69.40.0/24	172.29.40.0/23
5	N	C	9-16	201.69.50.0/24	172.29.50.0/23

Table 12.1: *Equipment and addresses for the final assignment.*

12.3 Security Guidelines

We shall imagine an enterprise scenario where we have to configure a network connecting two companies, A and B. Each team is configuring a company site, the number of sites being divided between the two companies.

The security guidelines are as follows:

- The internal computers should be able to connect to the internal FTP server.
- The computers from other sites belonging to the *same* company should be able to connect to the internal FTP server.
- The computers from other sites belonging to the *other* company should not be able to connect to the internal FTP server.
- The computers should be able to ping external hosts.
- It should not be possible for external hosts to ping internal computers.
- All computers should have Internet connectivity.

12.4 Device Configuration

We have to configure the following devices at each site.

- *Switch:* create the VLANs and assigning the corresponding ports.
- *Router:* configure the serial and Ethernet interfaces with the corresponding IP addresses, the routing protocol (RIPv1) and any needed static routes.
- *Access Point:* create a basic unsecured WLAN.
- *Firewall:* assign the IP addresses to the inside and outside interfaces, configure the DHCP server, security policy and NAT rules.

To configure the switch, you shall use an Ethernet port in VLAN 1[1]. To configure the router, you shall use the console connection. To configure the firewall and the access point, you shall use the Ethernet ports.

[1] Or alternatively, as your instructor may tell you.

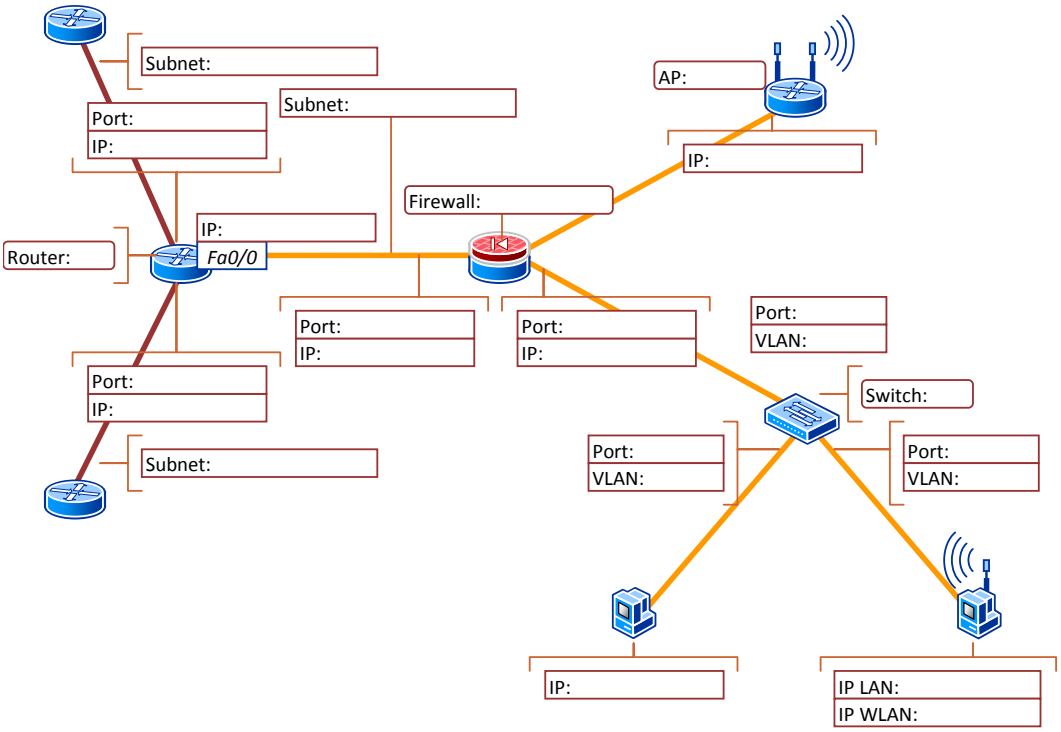

Figure 12.2: *Your configuration: equipments, ports and IP addresses.*

12.5 Home Preparation

Find which ranges of IP are private addresses. Find information about Classless Inter-Domain Routing (CIDR) and what is the difference between /23 and /24 networks.

Questions
Do the addresses assigned to WLAN and ethernet devices belong to the same subnetwork? Why?
What is the explanation for the IP address for the internal interface of the firewall?

Fill in the figure 12.2 with your configuration information.
Fill in the figure 12.3 with your configuration information.

12.6 Steps and Checkpoints for the Device Configuration

1. *Step:* Study the configuration.
2. *Checkpoint:* Complete the configuration information in the figures above.
3. *Step:* Configure the switches (VLANs and ports).
4. *Checkpoint:* Check that the VLANs were created and the ports assigned.
5. *Step:* Configure the internal wired computer and the firewall interfaces.
6. *Checkpoint:* Ping the firewall from the internal computer.
7. *Step:* Configure the router (interfaces and routing with RIP).

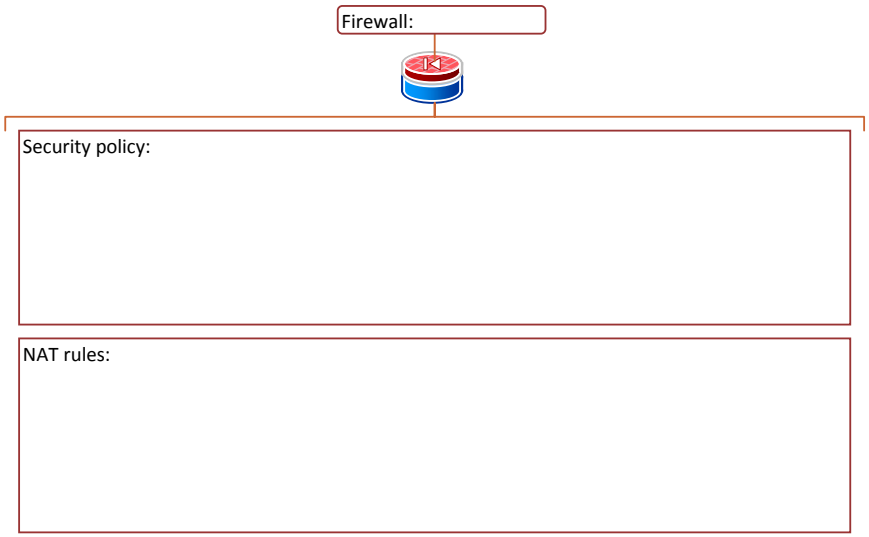

Figure 12.3: *Your firewall configuration: security policy and NAT rules.*

Switch	IP Address
Switch B	192.168.1.102
Switch C	192.168.1.103

Table 12.2: *The IP addresses of the lab switches.*

8. *Checkpoint:* Ping from the router to the firewall, ping between routers, routing table, ping between firewalls.
9. *Step:* Configure the firewall security policy and NAT rules.
10. *Checkpoint:* Ping from the internal LAN computer to the routers. Can connect to the FTP servers from the other sites of the same company.
11. *Step:* Configure the access point and firewall DHCP server.
12. *Checkpoint:* Connect the internal wireless computer to the WLAN, and receive the IP configuration.

12.6.1 Switch Configuration

The table 12.2 contains the IP addresses for the switches.

12.6.2 Computer Configuration

The IP address of the DNS server is 193.145.56.11. On your wired computer in the 172.29.X0.0/23 subnetwork, install and configure an FTP server, with the username `groupX` and password blank, where X is the number of your group.

12.6.3 Firewall Configuration

1. Connect the computer to the firewall on the *inside* interface.
2. Enable HTTPS access to the network 172.29.X0.0, where X is your group number.

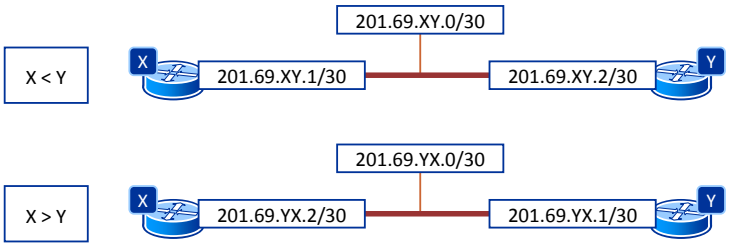

Figure 12.4: *The IP addresses for the serial interfaces of two routers belonging to the groups X and Y.*

3. Change the IP address of the *inside* interface to 172.29.X0.1/23. After this change you shall lose connectivity to the firewall.
4. Change the IP address of the computer to 172.29.X0.2/23. The default gateway is the *inside* interface of the firewall. Restart the ASDM.
5. Change the IP address of the *outside* interface of the firewall to 201.69.X0.1/24.
6. Add a static default route at the outside interface of the firewall with your router interface as a gateway.

12.6.4 Router Configuration

1. Configure the IP address of the Ethernet interface.
2. Configure the IP address of the serial interfaces. The IP addresses of a serial interfaces are assigned according to the figure 12.4. Do not forget to set the clock-rate to 128 000 for all DCE interfaces.
3. Add RIP to the routing configuration. Add all networks. After convergence, check the routing table.
4. Configure the Internet access. Add an static route to the gateway of the lab, having the IP address 192.168.1.1

12.6.5 Access Point Configuration

1. Change the IP of the access point and set the firewall as the default gateway.
2. Make sure that HTTP access is enabled.
3. Connect the access point to the firewall.
4. Use a computer with wired connection and the browser to connect to the access point. Configure the gateway. Configure the wireless network (enable the radio interface, SSID and security configuration).
5. Add a DHCP server to the firewall to provide an automatic configuration for the wireless computers. You can find the DHCP server configuration at Configuration >Properties >DHCP Services >DHCP Server. Configure the IP address range, the default gateway and the DNS.

12.6.6 Internet Gateway Configuration

The IP address of the lab Internet gateway (firewall) is 192.168.1.1/24.

12.7 Lab Report

The lab report should include the devices configuration and the validation tests. As a minimum, it should contain the following.

1. The figures 12.2 and 12.3 completed with the required information. You may download the fillable forms for your lab reports at the following links:
   - http://alex.bikfalvi.com/teaching/upf/2013/networks_and_services/lab/final/FormAddresses.pdf
   - http://alex.bikfalvi.com/teaching/upf/2013/networks_and_services/lab/final/FormFirewall.pdf
2. The configuration of the network equipments:
   - The running configuration of your (i) *router* and (ii) *switch*.
   - A snapshot of the firewall (i) *interfaces configuration*, (ii) *security policy*, (iii) *NAT rules* and (iv) *DHCP configuration*.
3. Tables with results of the following validation tests (perform these tests *after* all groups have finished their configuration):
   - Ping between your wired and wireless computers.
   - Ping from your wired and wireless computers to all other routers.
   - Ping from your router to your wired and wireless computers.
   - Connect to your FTP server from the wireless computer.
   - Connect from the wired and/or wireless computer to the FTP server of another site from your company.
   - Connect from the wired and/or wireless computer to the FTP server of another site from the other company.
   - Connect to the Internet.

12.8 Optional Assignments

Configure the firewall to prevent that wireless stations connect to the FTP server. Create a VPN between the sites of the same company.