COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

NETWORK SOLUTION FOR ACME MARKETING

Students:
Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

Supervisor:
Bent Buron

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

Table of Contents

IDENTIFIED REQUIREMENTS....3

ROLE OF THE NETWORKING DEVICES....8

INTERACTION AMONG THE NETWORKING DEVICES....10

IP ADDRESSING....11

BOTTLENECKS....13

SUFFICIENT BANDWIDTH....14

DEVICE CONFIGURATION....15

ACME....15

DMZ....19

FTP....22

SMART....24

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

IDENTIFIED REQUIREMENTS

- TCP/IP support w/ ip v4;

  This is a very basic setup requirement and is guaranteed to be met once you start assigning IPs, either via DHCP or statically. We have achieved this requirement fully.

- WIRED access

  Again, like the previous requirement, this forms the basis of networking, so no special effort was made to satisfy it, apart from simply drawing cable from one machine to another.

- TWO VLANs w/ separate communications

  We achieved this at first by creating two VLANs in the first switch we worked on. We then used Access Control Lists (ACLs, as we will be referring to them throughout the rest of this report) to achieve block access from one VLAN to the other. In order for this to work, we had to subnet the interface of the ACME router so as to allow two separate DHCP pools in the company. In the Packet Tracer simulation (we will be referring to this as "the simulation" for short for the rest of this article), we have met this requirement fully, as no host from department A can reach a host from department B, and vice-versa. The blocking itself is done via the ACL 120 in the ACME router.

- THREE FLOORS, each with access to the two vlans;

  This was perhaps one of the trickiest parts of the setup. The way we decided to do allows for easy movement of hosts from one floor to another and/or from one department to another, without the need for a specialized IT technician on premises to log into the equipment and change any other settings.

  The setup consists of multiple 16-port unmanaged switches spread across the three floors, along with one 10-port managed switch. We decided to go with 16-port switches because they allow for portability. Only the one managed switch is required to support VLAN tagging (the one called "SMART" in our simulation), while all the other could just be "dumb" (transparent) switches, with no support for VLAN tagging. This way you do

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

not have to spend that much money on the equipment. The average price for the expensive switch would be 180$[1] while the cheaper, "transparent" ones are around 70$[2]. The way this works is that all the VLAN (department) tagging is done at the SMART switch and all the other switches will be entirely either DEPT A or DEPT B, depending on the port they are connected to in the mother switch. So, the "SMART" switch will have the following setup:

one port - connection to ACME router;
one port - connection to WIFI AP;
two ports tagged for DEPT A;
the other six tagged for DEPT B;

Then, on each of the floors, you will place as many DEPT A or DEPT B switches as needed to handle the current distribution of employees. In the case where you need more than one switch per department per floor, you will need to connect the last-added switch for that department to the closest already set up switch for that department, in its route back to the "SMART" switch.

As an example, have a look at the following table:

FLOOR	SWITCHES A	SWITCHES B	TOTAL HOSTS PER FLOOR	TOTAL SWITCHES PER FLOOR
	(ports used/ports total)	(ports used/ports total)		
1	1 (3/16)	2 (19/29)	22	3
2	1 (10/15)	4 (47/57)	57	5
3	1 (7/15)	3 (34/43)	41	4

You can see that it would be really easy to have this setup working with only 13 switches (12 cheap ones and the "SMART" one). We cannot stress enough how important it is that the transfer of one hosts from one floor to another, or from one department to another, be as easy as possible. This will reduce time spent debugging network setup

[1] http://www.amazon.com/Cisco-SG300-10-10-port-Gigabit-SRW2008-K9-NA/dp/B0041ORN6U
[2] http://www.amazon.com/Cisco-SF100D-16-Port-Ethernet-Switch/dp/B003AVN1N4/

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

and increase the total productive of your employees, since they can get back to work almost immediately. In total, we recommend buying 13 of these "transparent" ones in order to have one in the reserve, just in case. Do note that this is just an orientative example that is not thoroughly optimized. I'm sure that once you know the exact number of hosts per department per floor, we can do some optimized version of this setup so as to have as few unused ports as possible. For example, we could make some of the B hosts on the ground floor connect directly to the SMART switch, and thus reduce the number of B switches on that floor.

And even though it may seem like wasteful to have so many ports not used, trust us when we say that this is preferable to the other way of having to deal with manually setting up the switches with the appropriate VLAN tags each time a host transfers.

This way any IT intern working at your company can easily move switches around according to the needs.

We have also done the calculations for another option. In this case we would suggest buying 8-port unmanaged switches instead of the 16-port ones. These are approx. 40$ each[3] and, if you were to buy 22 of them, like we suggest, would bring you at about the same total cost as the previous solution[4]. In this case, however, there would be fewer unused ports left over for each of them. We have prepared a table like the one before:

FLOOR	SWITCHES A	SWITCHES B	TOTAL HOSTS PER FLOOR	TOTAL SWITCHES PER FLOOR
	(ports used/ports total)	(ports used/ports total)		
1	1 (3/7)	3 (19/19)	22	4
2	2 (10/12)	8 (47/49)	57	10
3	1 (7/7)	6 (34/37)	41	7

[3] http://www.amazon.com/Cisco-SF100D-16-Port-Ethernet-Switch/dp/B003AVN1N4/
[4] About 900$ for the unmanaged ones, by our calculations.

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

However, this solution does not allow for rapid growth of your business. That is, in the case where you would hire a great new number of people, you would probably have to go out and buy some more.
In another note, you can always have peace of mind with most Cisco equipment because they offer Cisco Limited Lifetime Hardware Warranty.

- WEB SERVER, for guests, in a DMZ;
  - Each VLAN must have its own FILE SERVER that only hosts on that VLAN can access.
  - WEB & FILE SERVER are in a HOSTING DOMAIN;
  - SERIAL CONNECTION to the HOSTING DOMAIN;

  We basically fulfilled these requirements through the use of ACLs, again. In the matter of the FTP servers, we created a list that only allow access from the respective department's hosts and only on the ftp ports. The web server was more complex: we had to create a NAT binding between one of the public IPs available to us via the ISP to the internal IP of the WEB SERVER, on port 80 and 443. This way the WEB SERVER will only be exposed if the request comes over HTTP and to that specific IP. We chose 80.100.200.145 as the IP. The web server is also accessible from the internal network, by the employees, on the IP 10.10.10.13. The ACL reference is number 130 on the DMZ router.

- Access to PUBLIC INTERNET
  - Only one IP address should be used;

  This was done using NAT (Network Address Translation) overload, or, to be more precise, Port Address Translation (PAT). We set it up so that each host in the ACME domain would be allowed to access the public Internet by "overloading" the public IP assigned by the ISP to the DMZ router's public-facing interface. This was done to accommodate for the restriction of only using one public IP address. This type of solution is common-practice for economic reasons. Each host would be bound to a port instead of an entire IP, and this binding will be stored in the DMZ's router NAT table. In the example below, the internal host 192.168.20.13 will be bound to a port of the DMZ's public-facing Ethernet interface (1025) when reaching for the public Internet. We created

COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

list (number 1) to maintain the IP ranges that are allowed to use the PAT overloading on this router.

```
  route          IP routing table
  ssh            Information on SSH
DMZ#sh ip nat trans
DMZ#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 80.80.80.106:11   192.168.20.13:11   90.100.200.2:11    90.100.200.2:11
tcp 80.100.200.145:80  10.10.30.10:80     ---                ---
tcp 80.100.200.145:80  10.10.30.10:80     90.100.200.2:1025  90.100.200.2:1025
tcp 80.100.200.145:80  10.10.30.10:80     90.100.200.2:1026  90.100.200.2:1026
tcp 80.80.80.106:1025  192.168.20.13:1025 90.100.200.2:80    90.100.200.2:80
tcp 80.80.80.106:1026  192.168.20.13:1026 90.100.200.2:80    90.100.200.2:80
tcp 80.80.80.106:1027  192.168.20.13:1027 90.100.200.2:80    90.100.200.2:80
tcp 80.80.80.106:1028  192.168.20.13:1028 90.100.200.2:80    90.100.200.2:80
tcp 80.80.80.106:1029  192.168.20.13:1029 90.100.200.2:80    90.100.200.2:80
tcp 80.80.80.106:1030  192.168.20.13:1030 90.100.200.2:80    90.100.200.2:80
tcp 80.80.80.106:1031  192.168.20.13:1031 90.100.200.2:80    90.100.200.2:80
tcp 80.80.80.106:1032  192.168.20.13:1032 90.100.200.2:80    90.100.200.2:80
```

- Block access for the BAD GUYS;

Again, ACLs were the key. We simply denied all requests on the public-facing interface on the DMZ router that match the IP address of the "bad guys" server. We also blocked spoof attacks, where hackers forge packets faking an internal IP address. As per this RFC: https://tools.ietf.org/html/rfc4953. All of this went into the list numbered 105 on the DMZ router.

- WIFI access for guests;

-No ACCESS for these guests to the file server or to the department's hosts;

We granted WIFI access to the guests by simply adding an Access Point (AP) to the first switch connected to the ACME router. We created a separate DHCP pool and subnetted the router's interface once more. We then blocked any incoming request from this pool to the other departments of ACME (ACL 125 on ACME router). That way the guests have internet access without having access to the company's hosts. It was not necessary to add any additional ACLs in order to block access from the WIFI hosts to the FTP server, since the ACL on the DMZ allows only hosts from the respective departments.

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

ROLE OF THE NETWORKING DEVICES

We tried to make our network design as simple and functional as possible. Using the least amount of resources, money and devices.

ACME router:

- blocks access from one department to the other;
- blocks access from the wireless AP to the department hosts;
- allows access from the wireless AP to the public internet;
- assigns IPs via DHCP to the hosts in the departments, each department with its own subnet and pool;
- assigns IPs via DHCP to the wireless guest hosts. Also with its own subnet and pool;
- each DHCP pool is set to reserve some IP addresses, that won't be handed out to hosts.
- connects to the DMZ router in "Server Camping Inc." network;
- subdivides Fa0/0 in 4 sub-interfaces. Fa0/0.10, Fa0/0.20, Fa0/0.99 and Fa0/0.141. First one for Dept. A, second for Dept B, third for management (In case in the future Mr. Scrooge wants to hire a full-time IT expert, he can make use of this interface), and finally Fa0/0.141, for the guest WIFI network.

DMZ router:

- connects to the ACME router found on the client's premises;
- maintains access lists for the following:
  - 130: ingoing traffic to FTP servers, only allowing traffic from its respective department, and to the WEB server, only allowing traffic for HTTP and HTTPS;
  - 1: traffic to be assigned in the NAT pool, only allowing access from the web server and department hosts;
  - 105: controls incoming traffic to the interface exposed to the public internet, allowing everything but the badguys.com server, and incoming traffic spoofing internal IPs;
- maps the internal, private, static IP of the web server to one of the public available IPs granted by the ISP;
- makes use of one serial interface Se00 which is the DTE interface of the router-to-router serial connection between DMZ and ACME;
- makes use of one FastEthernet interface, Fa01, with its own subnet, that contains WEB and FTP servers

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

FTP switch:

- connects the DMZ router to the FTP servers and to the WEB SERVER;
- the WEB SERVER was deliberately placed behind the switch and not directly connected to the DMZ router, thus sparing the use of another interface on the DMZ router;

SMART switch:

- connects to ACME, to the Wireless AP, Floor1A, Floor1B, Floor2A and Floor2B switches;
- for simplicity reasons our packet tracer topology includes only one switch per department, per floor;
- has four ports configured for VLAN traffic:
  - Fa0/1 for VLAN 141, guest wireless AP
  - Fa0/4 is the trunk port connected to the ACME router;
  - Fa0/2 and Fa0/5 are marked for DEPT A;
  - Fa0/3, Fa0/6 to Fa0/10 are marked for DEPT B;

All the other switches in the ACME premises:

- have all their ports tagged as "access" for the default VLAN 1. This would be equivalent to being a "transparent", unmanaged switch without any understanding of VLANs at all.

Server FTPA:

FTP server for dept A;

- It's connected to the FTP switch on Fa0/3;

Server FTPB:

FTP server for dept B;

- It's connected to the FTP switch on Fa0/4;

Server0:

Web server that is made public through the DMZ router;

- It's connected to the FTP switch on Fa0/2;

Guest Wireless AP:

Access Point for guests in the lounge area.

- Only Web access and to the company's WEB SERVER. No access to any of the FTP servers or hosts;
- It's connected to the Main switch on Fa0/1;
- The port is tagged for traffic from VLAN 141, Guest Wireless VLAN;

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

INTERACTION AMONG THE NETWORKING DEVICES

ACME router:

- interacts with the hosts on the subnets of its FastEthernet0/0 interface by assigning IPs through DHCP and blocking access following certain rules;
- interacts with DMZ router through a serial connection;
- Interacts with wireless hotspot for guest host and mobile devices

DMZ router:

- interacts with the ISP by being a DHCP client on its Fa0/0 interface;
- interacts with ACME router via serial connection;
- control access to the DMZ resources (FTP and WEB) via the ACLs declared on it;
- blocks traffic to and from badguys.com;
- blocks incoming traffic that spoofs an internal IP, the localhost IP, or the broadcast IP (usual attack techniques);

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

IP ADDRESSING

hosts in DeptA - 192.168.10.11 to 192.168.10.255
IPs 192.168.10.1-10 are excluded from the dep. A DHCP pool.

hosts in DeptB - 192.168.20.11 to 192.168.20.255
IPs 192.168.20.1-10 are excluded from the dep. B DHCP pool.

hosts bound to the AP - 192.168.141.11 to 192.168.141.255
IPs 192.168.141.1-10 are excluded from the Wireless guest network DHCP pool.

DMZ has:
Fa0 /0 - 80.80.80.106 /24 (by DHCP on the ISP)
Fa0 /1- 10.10.10.1/24
Se0 /0 - 172.16.10.2/30

ACME has:
Fa0 /0.10 - 192.168.10.1/24
Fa0 /0.20 - 192.168.20.1/24
Fa0 /0.141 - 192.168.141.1/24
Fa0 /0.99 - 192.168.99.1/24
Se0 /0 - 172.16.10.1/30

WEB SERVER has:
Fa0 /0 - 10.10.10.13 static
80.100.200.145 (reachable from the outside network)

FTP A has:
Fa0 /0 - 10.10.10.11 static

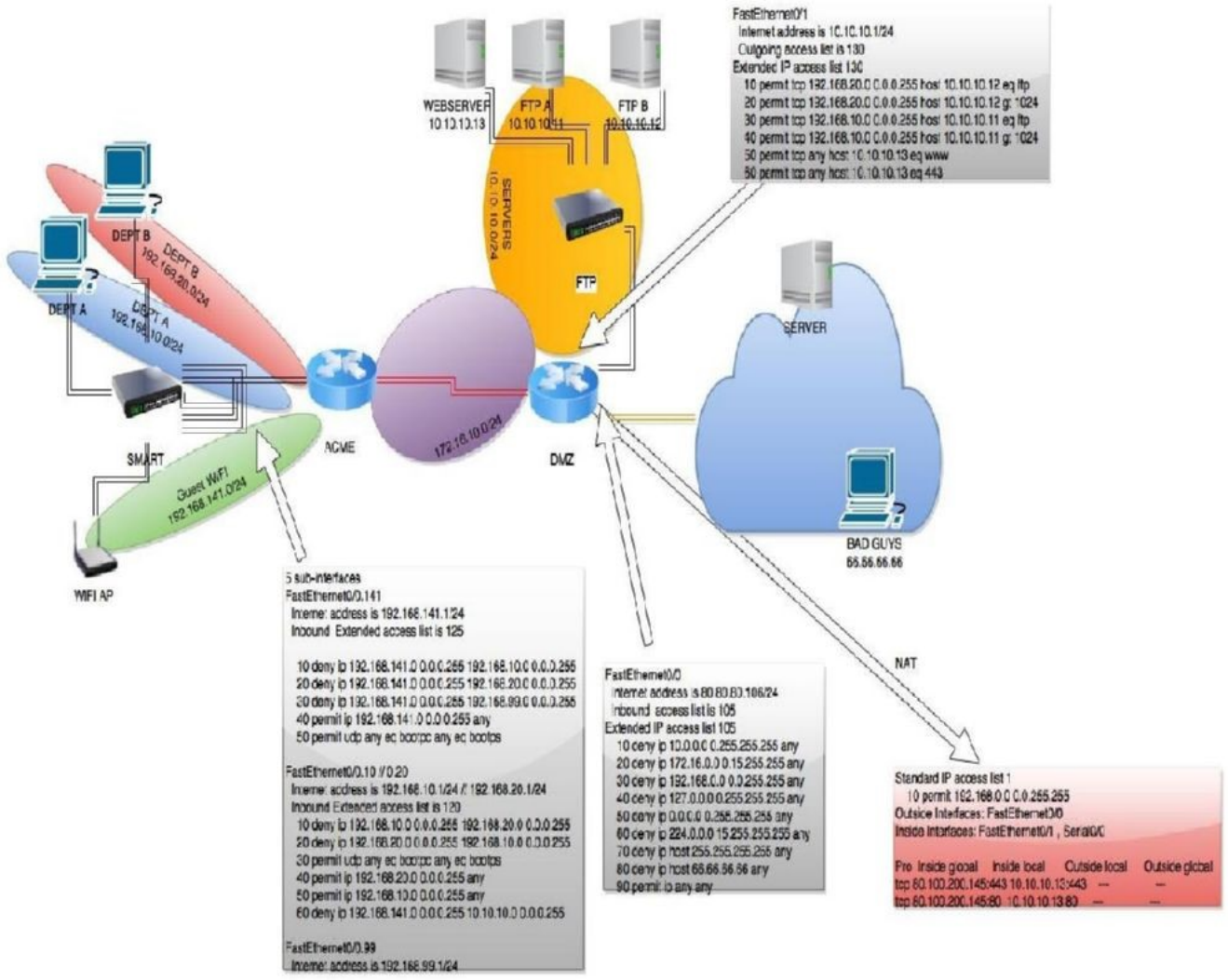
FTP B has:
Fa0 /0 - 10.10.10.12 static

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit



kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

BOTTLENECKS

From the information we have been provided by the company's representative we have learned that the following network traffic will be the norm:

300 MB/hour for the FTP servers;
187,5 MB/hour for WEB SERVER from the employees;
840 MB/hour for misc. traffic from the employees;

TOTAL: 1327.5 MB/hour

We were also told that the capacity of the serial connection between the ACME and the DMZ router will be 2 Mbps. Do note that this is in megabits not megabytes. And since one bit is one eighth of a byte, it means that the bandwidth will consist of 0,25 MB/second. Per hour that would mean 0,25 * 3600 = 900 MB. Therefore, it is easy to see that the serial connection between the company's site and the server camping network will be a bottleneck, reducing the productivity of the employees.

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

SUFFICIENT BANDWIDTH

We propose that you acquire a larger bandwidth from your internet provider. Something around your needs plus room for margin would be the ideal. We suggest either 1500 MB/hour (3.3 Mbps) or even 2000 MB/hour, to be on the safe side (4.4 Mbps).

Also, in case you would need to expand even further in the future, you might find yourself facing the same problem again.

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

DEVICE CONFIGURATION

ACME

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ACME
!
!
!
!
ip dhcp excluded-address 192.168.0.1 192.168.0.10
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
!
ip dhcp pool a
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.10.5
ip dhcp pool b
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.20.5
ip dhcp pool wifi
 network 192.168.141.0 255.255.255.0
 default-router 192.168.141.1
 dns-server 192.168.10.5
!
!
!
no ip cef
no ipv6 cef
!
```

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

```
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 no ip address
 shutdown
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip access-group 120 in
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip access-group 120 in
!
interface FastEthernet0/0.99
 encapsulation dot1Q 99
 ip address 192.168.99.1 255.255.255.0
```

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

```
 shutdown
!
interface FastEthernet0/0.141
 encapsulation dot1Q 141
 ip address 192.168.141.1 255.255.255.0
 ip access-group 125 in
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 172.16.10.1 255.255.255.252
!
interface Serial0/1
 no ip address
 clock rate 2000000
 shutdown
!
router rip
 network 172.16.0.0
 network 192.168.10.0
 network 192.168.20.0
 network 192.168.99.0
 network 192.168.141.0
!
ip classless
!
ip flow-export version 9
!
!
access-list 125 remark -- NO Guest Access to VLANs--
access-list 125 deny ip 192.168.141.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 125 deny ip 192.168.141.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 125 deny ip 192.168.141.0 0.0.0.255 192.168.99.0 0.0.0.255
access-list 125 remark -- Guest Access to Internet --
access-list 125 permit ip 192.168.141.0 0.0.0.255 any
```

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

```
access-list 125 remark -- ALLOW DHCP --
access-list 125 permit udp any eq bootpc any eq bootps
access-list 120 remark -- deny A to B and vice-versa --
access-list 120 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 120 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 remark -- ALLOW DHCP --
access-list 120 permit udp any eq bootpc any eq bootps
access-list 120 remark -- ALLOW INTERNET --
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
access-list 120 permit ip 192.168.10.0 0.0.0.255 any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

DMZ

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname DMZ
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
```

COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

```
 no ip address
!
interface FastEthernet0/0
 ip address dhcp
 ip access-group 105 in
 ip nat outside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.10.10.1 255.255.255.0
 ip access-group 130 out
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 172.16.10.2 255.255.255.252
 ip nat inside
 clock rate 56000
!
interface Serial0/1
 no ip address
 clock rate 2000000
 shutdown
!
router rip
 network 10.0.0.0
 network 80.0.0.0
 network 172.16.0.0
 default-information originate
!
ip nat inside source list 1 interface FastEthernet0/0 overload
ip nat inside source static tcp 10.10.10.13 80 80.100.200.145 80
ip nat inside source static tcp 10.10.10.13 443 80.100.200.145 443
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip flow-export version 9
```

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

```
!
!
access-list 130 remark -- DEPT A TO FTA, DEPTB TO FTPB --
access-list 130 permit tcp 192.168.20.0 0.0.0.255 host 10.10.10.12 eq ftp
access-list 130 permit tcp 192.168.20.0 0.0.0.255 host 10.10.10.12 gt 1024
access-list 130 permit tcp 192.168.10.0 0.0.0.255 host 10.10.10.11 eq ftp
access-list 130 permit tcp 192.168.10.0 0.0.0.255 host 10.10.10.11 gt 1024
access-list 130 remark -- only allow http and https traffic to web server --
access-list 130 permit tcp any host 10.10.10.13 eq www
access-list 130 permit tcp any host 10.10.10.13 eq 443
access-list 1 remark -- NAT list permissions --
access-list 1 permit 192.168.0.0 0.0.255.255
access-list 105 remark - block attacks spoofing internal IPs -
access-list 105 deny ip 10.0.0.0 0.255.255.255 any
access-list 105 deny ip 172.16.0.0 0.15.255.255 any
access-list 105 deny ip 192.168.0.0 0.0.255.255 any
access-list 105 remark -- block localhost spoofing --
access-list 105 deny ip 127.0.0.0 0.255.255.255 any
access-list 105 deny ip 0.0.0.0 0.255.255.255 any
access-list 105 remark - private multicast + broadcast -
access-list 105 deny ip 224.0.0.0 15.255.255.255 any
access-list 105 deny ip host 255.255.255.255 any
access-list 105 remark - block badguys.com -
access-list 105 deny ip host 66.66.66.66 any
access-list 105 permit ip any any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
```

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

end

COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

FTP

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname FTP
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
```

COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

```
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
```

COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

```
 login
!
!
end
```

SMART

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SMART
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 141
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
!
interface FastEthernet0/4
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
```

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

```
!
interface FastEthernet0/7
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode trunk
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
```

COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit

```
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface Vlan1
 no ip address
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

kea
COPENHAGEN SCHOOL OF
DESIGN AND TECHNOLOGY

Cristian Mitroi
Ruben Lisboa
Saem Samarnmit