Technische Universität Braunschweig
Institut für Betriebssysteme und Rechnerverbund

Computer Networks Administration
Help Manual

Sana Saadaoui Jemai | Oliver Wellnitz

Braunschweig, 27th March 2007

Contents

1. IP addresses allocation

This section presents a guide to IP Subnet Addressing. It shall help you when allocating IP addresses to the different hosts, routers and Web servers in office 1 and office 2.

1.1. *Subnet Sheet*

	Hosts	Netmask
/30	4	255.255.255.252
/29	8	255.255.255.248
/28	16	255.255.255.240
/27	32	255.255.255.224
/26	64	255.255.255.192
/25	128	255.255.255.128
/24	256	255.255.255.0

1.2. *Guide to sub-class blocks*

/25 -- 2 Subnets -- 126 Hosts/Subnet

Network #	IP Range	Broadcast
.0	.1-.126	.127
.128	.129-.254	.255

/26 -- 4 Subnets -- 62 Hosts/Subnet

Network #	IP Range	Broadcast
.0	.1-.62	.63
.64	.65-.126	.127
.128	.129-.190	.191
.192	.193-.254	.255

/27 -- 8 Subnets -- 30 Hosts/Subnet

Network #	IP Range	Broadcast
.0	.1-.30	.31
.32	.33-.62	.63
.64	.65-.94	.95
.96	.97-.126	.127
.128	.129-.158	.159
.160	.161-.190	.191
.192	.193-.222	.223
.224	.225-.254	.255

/28 -- 16 Subnets -- 14 Hosts/Subnet

Network #	IP Range	Broadcast
.0	.1-.14	.15
.16	.17-.30	.31
.32	.33-.46	.47
.48	.49-.62	.63
.64	.65-.78	.79
.80	.81-.94	.95
.96	.97-.110	.111
.112	.113-.126	.127
.128	.129-.142	.143
.144	.145-.158	.159
.160	.161-.174	.175
.176	.177-.190	.191
.192	.193-.206	.207
.208	.209-.222	.223
.224	.225-.238	.239
.240	.241-.254	.255

/29 -- 32 Subnets -- 6 Hosts/Subnet

Network #	IP Range	Broadcast
.0	.1-.6	.7
.8	.9-.14	.15
.16	.17-.22	.23
.24	.25-.30	.31
.32	.33-.38	.39
.40	.41-.46	.47
.48	.49-.54	.55
.56	.57-.62	.63
.64	.65-.70	.71
.72	.73-.78	.79
.80	.81-.86	.87
.88	.89-.94	.95
.96	.97-.102	.103
.104	.105-.110	.111
.112	.113-.118	.119
.120	.121-.126	.127
.128	.129-.134	.135
.136	.137-.142	.143
.144	.145-.150	.151
.152	.153-.158	.159
.160	.161-.166	.167
.168	.169-.174	.175
.176	.177-.182	.183
.184	.185-.190	.191
.192	.193-.198	.199
.200	.201-.206	.207
.208	.209-.214	.215
.216	.217-.222	.223
.224	.225-.230	.231
.232	.233-.238	.239
.240	.241-.246	.247
.248	.249-.254	.255

/30 -- 64 Subnets -- 2 Hosts/Subnet

Network #	IP Range	Broadcast
.0	.1-.2	.3
.4	.5-.6	.7
.8	.9-.10	.11
.12	.13-.14	.15
.16	.17-.18	.19
.20	.21-.22	.23
.24	.25-.26	.27
.28	.29-.30	.31
.32	.33-.34	.35
.36	.37-.38	.39
.40	.41-.42	.43
.44	.45-.46	.47
.48	.49-.50	.51
.52	.53-.54	.55
.56	.57-.58	.59
.60	.61-.62	.63
.64	.65-.66	.67
.68	.69-.70	.71
.72	.73-.74	.75
.76	.77-.78	.79
.80	.81-.82	.83
.84	.85-.86	.87
.88	.89-.90	.91
.92	.93-.94	.95
.96	.97-.98	.99
.100	.101-.102	.103
.104	.105-.106	.107
.108	.109-.110	.111
.112	.113-.114	.115
.116	.117-.118	.119
.120	.121-.122	.123
.124	.125-.126	.127
.128	.129-.130	.131
.132	.133-.134	.135
.136	.137-.138	.139
.140	.141-.142	.143
.144	.145-.146	.147

.148	.149-.150	.151
.152	.153-.154	.155
.156	.157-.158	.159
.160	.161-.162	.163
.164	.165-.166	.167
.168	.169-.170	.171
.172	.173-.174	.175
.176	.177-.178	.179
.180	.181-.182	.183
.184	.185-.186	.187
.188	.189-.190	.191
.192	.193-.194	.195
.196	.197-.198	.199
.200	.201-.202	.203

.204	.205-.206	.207
.208	.209-.210	.211
.212	.213-.214	.215
.216	.217-.218	.219
.220	.221-.222	.223
.224	.225-.226	.227
.228	.229-.230	.231
.232	.233-.234	.235
.236	.237-.238	.239
.240	.241-.242	.243
.244	.245-.246	.247
.248	.249-.250	.251
.252	.253-.254	.255

2. Access to the machines

This section describes the steps you have to perform in order to access all the machines involved in this practicum. You will have to deal with hardware routers (Juniper J2300, Cisco 2610), switches (Nortel BayStack 450-24T), physical computers and virtual machines.
The machines are located in the network laboratory Room 152 and must be remotely configured from the CIP Pool in Room G40. You should issue the following instructions each time you want to connect to one of the listed machines,

2.1. *Access to the virtual routers and Web servers*

- Find out on the Web interface the physical computer to which the virtual machines are connected. Refer to the URL: https://www.ibr.cs.tu-bs.de/vhm/
- Login to this computer with the command **"ssh"**. E.g. ssh milkyway.ibr.cs-tu.bs.de
- Give your own password.
- You can have access to:
  - PacX-router1: Router on office 1
  - PacX-www1: Web server on office 1
  - PacX-router2: Router on office 2
  - PacX-www2: Web server on office 2

  X is your group number.
- Login with the user "root" and password "pac07ibr"
- Press **"Strg+]"** to logout. For the Apple computers, "]" is obtained by combining the tabs **"ALT+6"**

2.2. *Access to the Juniper/Cisco Routers*

- To remotely access the physical routers (Juniper/Cisco), execute the command "telnet labconsole 1000X"; X is your group number.
- Press **"Strg+]"** and execute the **"mode character"** to disable the line mode (enter the character mode)

2.3. *Access to the Switch*

- Use the command "telnet labconsole 10010" to connect to the switch.
- Enter the character mode.

3. Configuration tools

We deal in this section with the configuration of the virtual machines. The section refers only to the virtual PCs and does not invoke the hardware routers. Configuration examples for these routers are provided in the next section (section 4).
All the virtual machines use Debian Linux. As a network administrator, you must handle all aspects of the network configuration in your company. For this purpose, we present in the following some networking configuration tools necessary for network configuration management in a Debian Linux environment.

3.1. *Network configuration management*

The main network configuration file is **"/etc/network/interfaces"**. It describes various aspects of the network management system and contains different stanzas identified by "iface", "auto" and "mapping".
Help: man interfaces.
The directive **"iface"** describes an interface configuration. It takes three arguments:

- *name*
  The name of the configuration (e.g. eth0).
- *address family*
  The network address family (e.g. inet)
- *method*
  The configuration method (e.g. static or dhcp)

Tools: *ifconfig, route, netstat, ip*
Help: man <tool>.

3.2. *Bringing up/down network interfaces*

Network interfaces are controlled by the two commands ***"ifup/ifdown"***
Syntax: ifup <if> ⟶ *brings up a network interface.*
Ifdown <if> ⟶ *takes an interface down.*

3.3. *Enabling IP forwarding*

As its name indicates, *IP forwarding* enables machines to forward packets. In Linux, *IP forwarding* is generally disabled. This option must be turned on in a Linux computer if you intend to use it as a gateway or router. Hence, you have to activate *IP forwarding* in your software routers. Otherwise, they are incapable of forwarding packets.
The configuration files are:

- /proc/sys/net/ipvt/ip_forward
- /proc/sys/net/ipvt/conf/<netif>/forwarding

The Debian system allows the administrator to manage a number of aspects of the network subsystem. Among others, the following options can be controlled:

- *IP forwarding:* As mentioned above, it enables a local machine to route packets between interfaces.
- *Spoof protection (rp_filter):* ensures that packets are accepted on an interface only if the correspondent response packets leave the machine through the same interface.

These options can be enabled via sysctl file **"/etc/sysctl.conf".**
Help: man sysctl.

3.4. *IP Tunnel configuration*

To configure an IP Tunnel on the software routers, you can issue the following commands in the main network configuration file **"/etc/network/interfaces"**.

ip tunnel add tunnel_name ***mode*** (gre, ipip) ***local*** IP@ ***remote*** IP@ ***ttl 64***

You also have to create a new network interface for the tunnel:

auto tunnel_name

iface ….

4. Configuration examples

We provide in this section some configuration examples for the two hardware routers Cisco and Juniper. More details about the two routers and their configurations can be found in their online documentations. The correspondent web references are:

- http://www.cisco.com for the Cisco router 2610, Cisco IOS
- http://www.juniper.net for the Juniper J2300, JunOS

4.1. *Interface configuration*

Cisco Configuration:

A Cisco router command-line-interface provides different modes. Each mode corresponds to a configuration range and is distinguished by its set of available commands. The mode you are in determines the commands you can use.

When you first connect to the router, you enter the *EXEC mode* (Prompt: `Router>`). To configure the router, you must switch to the *privileged mode* (Prompt: `Router#`) by executing the command:

`enable`

`"show ?"` displays the show commands available for a given mode. E.g. in the *privileged mode*, you can display the current configuration of the router by:

`show running-config`

To configure new features of the router, you must enter the *global configuration mode* (Prompt: `Router(config)#`). You issue the command:

`configure terminal`

To configure a new interface, you must switch from the *global configuration mode* to the *interface configuration mode* (Prompt: Router`(config-if)#`). Execute the command:

`interface <type> <slot>/<port>` (E.g. interface FastEthernet 0/0)

In the *interface configuration mode*, the following commands can be executed:

`Shutdown`	causes an interface to be administratively down.
`no shutdown`	activates an interface
`ip address <ip address> <netmask>`	configures the IP address and the netmask of the correspondent interface.

To return to the upper mode, you execute **`"exit".`** With **`"crtl+c"`**, you can directly go back to the parent privileged mode.

In the privileged mode, you can selectively display the configuration of a given interface with:

`show running-config interface <type> <slot>/<port>`

Juniper Configuration:

Once logged to the juniper router (with the User "root" and password "pac07ibr"), you can activate the command-line-interface by executing:

```
cli
```

At this step, you are at the privileged mode of the router (Prompt: `Router>`). To display the current configuration, you must issue the command:
Show configuration
To modify any configuration feature, you must enter the configuration mode (Prompt: `Router#`) by executing:

```
configure
```

The entire configuration follows a tree hierarchy. To modify a statement, you execute:

```
edit <statement> [<sub-statement>] […]
```

At a given hierarchy level, you can enter statements in any order. The command edit is used to move inside a specified statement hierarchy by indicating its path.
Syntax: edit statement-path.

To move up one level in the statement hierarchy, you can execute:

```
Up
```

To display the current configuration at a hierarchy level, execute:

```
show
```

to configure an interface, move inside the tree Interfaces <if-name> unitX family inet and set the IP address with:

```
set address <ip address>/<prefix length>
```

The command set is used to create a new configuration object and set its value.
To delete an identifier value, use the command

```
delete
```

Any change you introduce does not have an operational effect on the running configuration. To commit your modifications, you must issue the command:

```
commit
```

4.2. ***Static routes configuration***

Cisco Configuration:

In the global configuration mode of a Cisco router (Prompt: `Router(config)#`), you can set a static route with the following instruction:

```
ip route <destination prefix> <destination mask> <next-hop>
```

All arriving packets to the network having the Address <*destination prefix*> and the Netmask <*destination mask*>, are forwarded to the IP address <*next-hop*>.

Juniper Configuration:

In the configuration mode (Prompt: `Router#`), you can set a static route with the command:

```
set routing-options static route <destination> next-hop <next-hop ip>
```

Incoming packets to the network described by the address <*destination*> are forwarded to the IP address <*next-hop ip*>. The network address <destination> must be in CIDR-Notation (E.g. 172.16.2.128/26).

4.3. *Vlan configuration*

To assign several VLANs to a physical interface (E.g. fe 0/0), logical interfaces must be configured on the hardware routers (Cisco: sub-interfaces, Juniper: units). Similar to physical interfaces, you can allocate IP addresses to logical interfaces.

Cisco Configuration:

The following configuration assigns a new sub-interface FastEthernet0/0.130 to the physical interface FastEthernet0/0. The outgoing frames are tagged with the VLAN-ID 130.

```
Interface FastEthernet0/0.130
      encapsulation dot1Q 130
      ip address 172.16.0.10 255.255.255.252
```

Juniper Configuration:

In a Juniper router, a logical interface can be created with the command **`unit`**. The VLAN-ID is specified with the instruction **`vlan-id`**. The following example describes a new unit assigned to the physical interface **`fe-0/0/0.`**

```
Interfaces {
      fe-0/0/0{
            vlan-tagging;
            unit 120 {
                  vlan-id 120;
                  family inet {
                        address 172.16.0.6/30;
                  }
            }
}
```

4.4. *Dynamic routing protocol "RIP"*

RIP is a "Distance Vector" routing protocol. It is based on an algorithm that uses distance vector to compare routes and identify the best path to a given destination address. Each router maintains a routing table containing one entry for each router in the same subnet. This entry includes in terms two parts: The outgoing line to use for that destination address and an estimate of the distance to that destination.

By exchanging routing tables with its neighbors, a router finds out the neighbor to which it must forward a coming packet with a given destination address (the neighbor that offers the best estimate to that address). Further information about the RIP Protocol can be found in:

- Lecture Kommunikationssysteme
- Andrew S. Tannenbaum: "Computer Networks", Fourth Edition, 2003
- RFC 1721

To enable the dynamic routing protocol RIP on the hardware routers (Cisco, Juniper), you must insert new configuration instructions on each router.

Cisco Configuration:

For the Cisco router, you have only to indicate the RIP version and the network the protocol will route for. The following example describes a RIP configuration.

```
router rip
version 2
network 172.16.3.128 (without Netmask)
```

Juniper Configuration:

For the Juniper router, you have to indicate the interfaces which are RIP enabled. You must also explicitly define an export policy and indicate in the RIP configuration with the instruction **"export"**, that the policy will be applied. Without such policies routes learned from a certain RIP neighbor would not be further advertised to other RIP neighbors ("no redistribution").

```
policy-options {
      policy-statement <policy-name> {
            from protocol rip;
            then accept;
      }
}
protocols {
      rip {
            group rip {
                  export <policy-name>;
                  neighbor fe-0/0/0;
            }
      }
}
```

4.5. *Dynamic routing "OSPF"*

OSPF (Open Shortest Path First) is a Link State Routing Protocol. OSPF operates by representing actual networks, routers and lines with an arc graph in which each arc is assigned a cost. Based on the weights of the arcs, OSPF determines the least-cost path and chooses it as the best path.

OSPF allows ASes in the Internet to be subdivided into numbered areas (networks). All areas in an AS are connected to a backbone area called area 0. Within this hierarchy, OSPF distinguishes four classes of routers:

- *Internal routers:* are routers within a given area
- *Backbone routers:* are routers within the backbone area.
- *Area Border routers*: are routers connecting two or more areas.

- *AS Boundary routers:* are routers that belong to a given AS and that communicate with other routers in a different AS.

In OSPF, information is exchanged between adjacent routers. Each router collects Link State advertisements of all its adjacent routers and maintains a database that describes the entire AS topology. Participating routers periodically flood Link State Update messages throughout the AS to distribute their local state (their usable interfaces and reachable neighbor) and provide their costs.
OSPF does not send its routing information using UDP or TCP. It uses raw IP datagams instead. OSPF defines five message types:

- *Hello:* these messages allow a router to discover other adjacent routers.
- *Database Description:* convey the content of the Link State database from one router to another.
- *Link State Request:* allow a router to request update information from another router.
- *Link State Update*: are sent in response to a link state request and provide the router's local state and cost.
- *Link State Acknowledgement:* acknowledge the Link State Update messages.

Further information concerning the OSPF routing protocol can be found in:

- Lecture Kommunikationssysteme
- RFC 2328
- Andrew S. Tannenbaum: "Computer Networks", Fourth Edition, 2003

The following examples describe an OSPF configuration on the hardware routers (Cisco, Juniper)

Cisco Configuration:

The OSPF configuration process is quite simple. OSPF is enabled by creating an OSPF routing process and specifying a process ID. Different OSPF processes are allowed on the same router, but each with a different process ID. For a basic OSPF configuration, it is sufficient to define the interfaces on which OSPF runs and to specify the area to which they belong.
For example for the interfaces of the network 192.94.8.0/24 in the area 0.0.0.0, you issue:

```
router ospf <process-id>
      network 192.94.8.0 255.255.255.0 area 0.0.0.0
```

If you want to summarize routes being advertised from one OSPF area to another on an Area Border, we use the command **`area range`**. For example if you want to summarize all routes within the area 0.0.0.0 for the block 192.94.8.0/24, you execute the instruction:

```
area 0.0.0.0 range 192.94.8.0 255.255.255.0
```

Finally, you have to set the cost on each relevant interface. The OSPF cost is incorporated in the calculation of the best routes. It specifies the cost of sending a packet on an OSPF interface. E.g. To assign the OSPF cost 50 to an interface, you can use the following instruction in the interface configuration mode:

```
Router(config-if)# ip ospf cost 50
```

Juniper Configuration:

The following example presents an OSPF configuration on a Juniper router:

```
protocols {
```

```
      ospf {
            area 0.0.0.0 {
                  area-range 192.94.8.0/24;
                  interface fe-0/0/0.0;
            }
      }
}
```

Similar to Cisco routers, OSPF costs are assigned to interfaces to specify the cost of sending a packet on a given interface. The following instruction sets an OSPF cost:

```
set protocols ospf area 0.0.0.0 interface fe-0/0/0.0 metric <cost>
```

4.6. *Inter-Domain Routing "BGP"*

The Internet is made up of a large number of independent sub-networks (approximately 20000) called Autonomous Systems (AS). In order to ensure world wide accessibility to the WWW, these sub-networks are interconnected and exchange routing information. We distinguish two kinds of routing protocols:

Interior Gateway Protocols (IGP): are used within a single AS. An Interior Gateway Protocol has to transmit packets as efficiently as possible from a source to a destination. The emphasis is therefore on the efficient use of the own network. Well known protocols in this category are OSPF and RIP.

Exterior Gateway Protocols (EGP): are used between ASes. The so-called BGP (Border Gateway Protocol) is the most famous. For Exterior Gateway Protocols in general and BGP in particular, a great stress is put on routing policies. This constitutes the main difference to Interior Gateway Protocols such as OSPF and RIP. Typical policies take into account economic or security considerations: Which routing information is exchanged and which is not, first specified in contracts between the ASes and then manually configured into BGP routers.

BGP is a "Distance Vector Protocol" but quite different from most routing protocols belonging to this category. A BGP router keeps track of the path used to reach each destination. Instead of communicating the estimated cost to each possible destination, it tells its neighbours the exact path it is using. Each BGP router selects then the route with the shortest path. To ensure a reliable communication, BGP routers establish TCP connections to communicate with each other.

Further information about BGP routing can be found in:

- RFC 1771 to 1774
- Andrew S. Tannenbaum: "Computer Networks", Fourth Edition, 2003

Examples of BGP configuration on the hardware routers (Cisco and Juniper) are provided in the following.

Cisco Configuration:

A BGP configuration is initiated by creating a BGP-Process and defining the AS to which it belongs.

```
router bgp <AS-Number>
```

More information about the BGP routing protocol can be found in this Cisco documentation:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/iprrp_r/ip2_00g.htm

BGP employs many policy control techniques. The following example describes a basic configuration using *"Route-Maps"*. In this example, all routes learned by the neighbor 1.2.3.4 and whose *AS-Path* contains AS 3456 are assigned a *Local-Preference* value 100. All remaining routes of the neighbor 1.2.3.4 get the *Local-preference* value 200. For a router in the AS 3549, such configuration looks like:

```
router bgp 3549
```

```
! [...]
      neighbor 1.2.3.4 route-map my_policy in
!
ip as-path access-list 1 permit 3456
!
route-map my_policy permit 10
      match as-path 1
      set local-preference 100
!
route-map my_policy permit 20
      set local-preference 200
```

If a match condition is not indicated within the route-map, then the rule is automatically applied to all paths. Otherwise, you can explicitly define an AS-Path to which the rule will be applied. The command ip as-path access-list is used for this purpose. You can refer to the above URL for more details.
Another important clue is that certain updates such as *Local_Preference* don't become effective unless the BGP session is reset with the command:

```
clear ip bgp
```

Juniper Configuration:

A summary of all BGP configuration commands for the Juniper router is available in this URL:
http://www.juniper.net/techpubs/software/junos/junos70/swconfig70-routing/html/bgp-config.html
You can find out a basic BGP configuration in the section *"Minimum BGP Configuration"*
Bear in mind that you can create for each neighbor its own group. A BGP neighbor group is formed by two or more neighbors that share a common set of policies. This has the advantage that you can specify for each neighbor a different set of policies.
You can refer to the following URL for details about policies configuration.
http://www.juniper.net/techpubs/software/junos/junos70/swconfig70-policy/html/policy-framework-summary10.html

A *Policy* configuration includes two steps. First you have to define a *Policy* by introducing a *policy-statement* in the hierarchy level *policy-options.*
For example you can define a policy and set a *Local-Preference* value 200 for all *AS-Paths* that contain AS 3456, as follows:

```
policy-options {
      policy-statement my_policy {
            from {
                  protocol bgp;
                  as-path my_reg_expr;
            }
            then {
                  local-preference 200;
            }
      }
      as-path my_reg_expr "3456";
}
```

In the second step, you must specify to which BGP neighbour the policy will be applied. This can be achieved using an export/import statement within the appropriate hierarchy level of the BGP configuration. You can refer to the section "Configuring BGP Routing Policy" in the Juniper documentation (above URL) for more details. Bear in mind here also that certain changes such as *Local_Preference* become effective only if the BGP session is reset.

```
clear bgp neighbor
```

5. Network diagrams

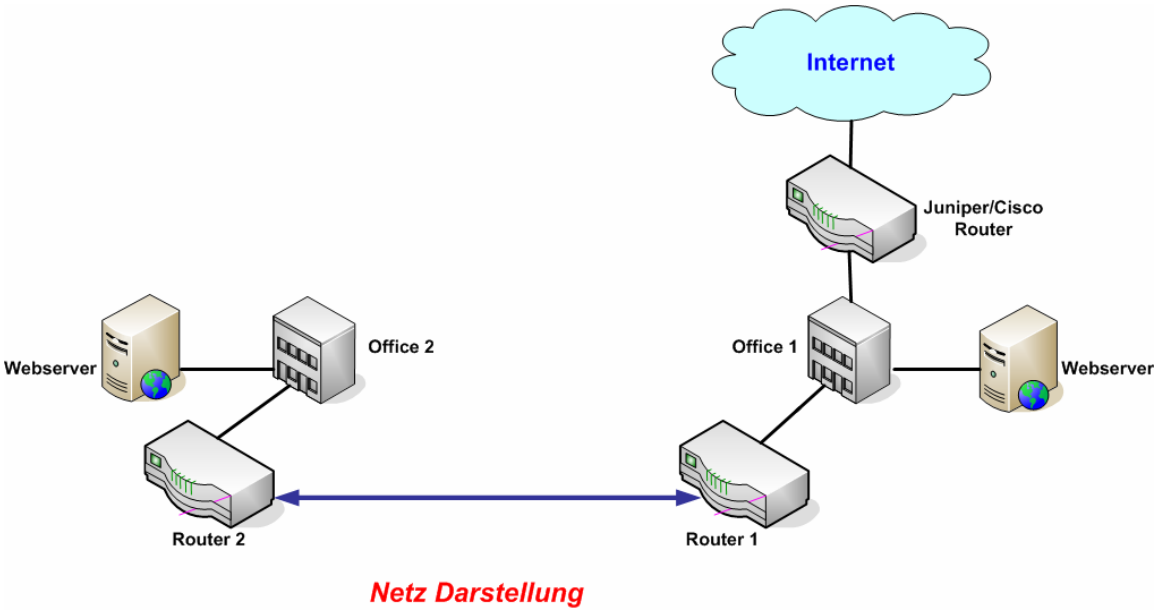

Figure 1: Network Diagram

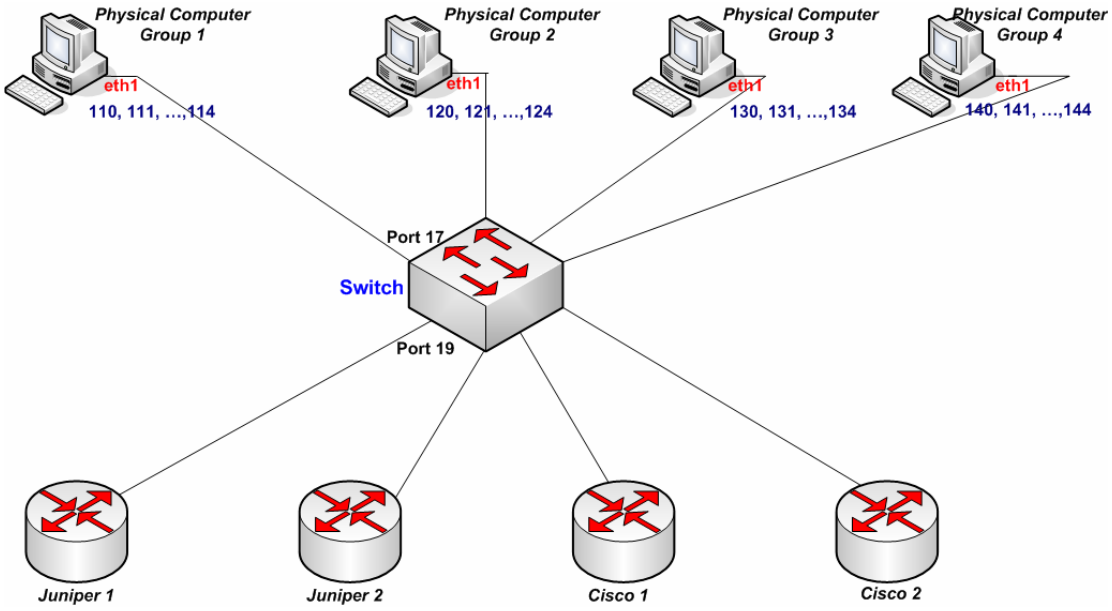

Figure2: VLAN Scenario