Student notes for

David Bombal's

Packet Tracer
Labs Course

David Bombal

THANK YOU!

These student notes have been kindly shared by @DJninjaNZ

Thank you @DJninjaNZ for sharing! Please also give your thanks to @DJninjaNZvia Twitter.

These are not official student notes and are not officially supported, but are shared with the hope that they will help you with your CCNA studies.

If you want to share your notes with others on the course, please submit them to sales@ConfigureTerminal.com and we will review them for addition to the course.

Remember: You will probably learn more by making notes like these and sharing them for the benefit of others.

All the best!

David Bombal

DISCLAIMER:

The contents in these student notes are the work and copyright of @DJninjaNZ and are designed to assist candidates in the preparation for Cisco Systems' CCNA certification exams. While every effort has been made to ensure that all material isas complete and accurate as possible, the enclosed material is presented on an "as is" basis. Neither the authors nor Network Experts Internet Ltd, assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in these notes.

These notes were developed by @DJninjaNZ, and is an original work of the aforementioned authors. Any similarities between material presented in these notes and the actual CCNA exam material is completely coincidental.

Cisco®, Cisco Systems®, CCIE, CCNA, CCENT, and Cisco Certified Internetwork Expert, are registered trademarks of Cisco Systems, Inc., and its affiliates in the United States and certain countries.

All other products and company names mentioned in these notes are the trademarks, registered trademarks, and service marks of the respective owners.

Contents

Brief

This lab is for configuring the basic campus network using VTP and access/trunk ports

Lab requirements

Configure the network as follows:

Lab: Configuring PPP with CHAP and Extra real-world applications

Required Tasks:
1. Power on devices and then configure the devices as follows:
2. Configure IP addresses as shown in the diagram
3. Ensure routers can ping each other
4. Configure an enable password of "cisco"
5. Encrypt the enable password
6. Configure a secret password of "cisco123"
7. Configure the first 5 telnet lines and use a line password of cisco on them
8. Make sure you can telnet from one device to the other
9. Configure a console password of "cisco" and test

Vlan Intercommunication

- This lab is like the last lab with more Vlans and devices but this time also the switches are configured to be on a management Vlan which is practical in the real world.
- Best practice is not to use Vlan 1.
- Like previously configure pc ports connected to switches as access (This includes g1/0/20 connected to the server) and switch ports to switch as trunk.
- Configuring the 3650-switch layer 3 switch with IP addresses and interVlan routing
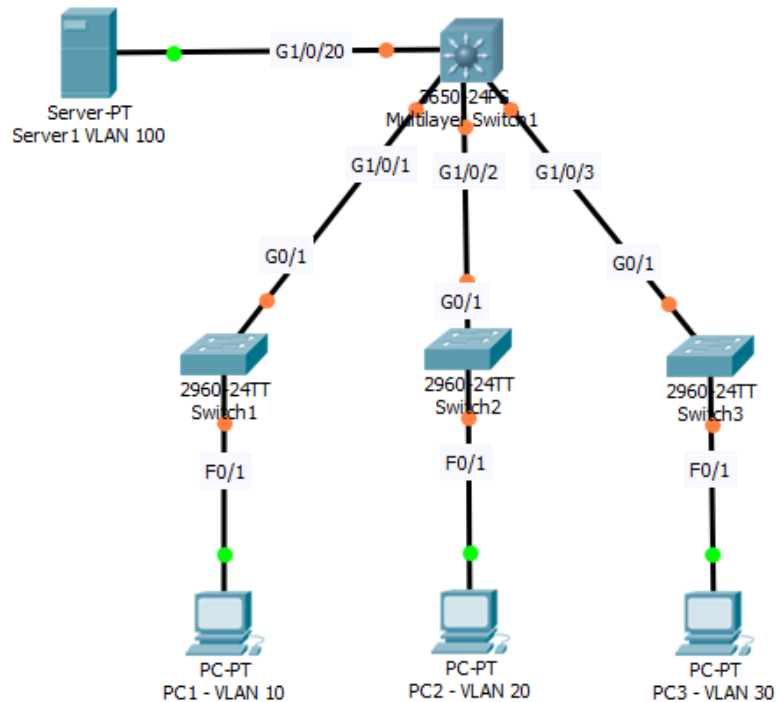
3

Lab Topology

Figure 1

Here we have a campus network with four Vlans configured and one for management all the configurations will be done on the switches this lab contains no routers. The multi-layer switch can be used as a router when routing is enabled.

Configurations and Verification

```
Campus Network


Core
!
ip routing
!
interface GigabitEthernet1/0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchportnonegotiate
!
interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchportnonegotiate
!
interface GigabitEthernet1/0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchportnonegotiate
!
```

```
interface GigabitEthernet1/0/20
switchport access vlan 100
switchport mode access
switchportnonegotiate
!
interface Vlan1
ip address 10.1.1.254 255.255.255.0
!
interface Vlan10
mac-address 0090.219d.7001 //auto generated
ip address 10.1.10.254 255.255.255.0
!
interface Vlan20
mac-address 0090.219d.7002
ip address 10.1.20.254 255.255.255.0
!
interface Vlan30
mac-address 0090.219d.7003 //auto generated
ip address 10.1.30.254 255.255.255.0
!
interface Vlan100
mac-address 0090.219d.7004 //auto generated
ip address 10.1.100.254 255.255.255.0
!
```

S1
```
!
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
!
interface GigabitEthernet0/1
switchport mode trunk
!
!
interface Vlan1
ip address 10.1.1.1 255.255.255.0
!
ip default-gateway 10.1.1.254
```

S2
```
!
interface FastEthernet0/1
switchport access vlan 20
switchport mode access
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 10.1.1.2 255.255.255.0
!
ip default-gateway 10.1.1.254
!
```

S3
```
!
interface FastEthernet0/1
switchport access vlan 30
```

5

```
switchport mode access
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface Vlan1
ip address 10.1.1.3 255.255.255.0
!
ip default-gateway 10.1.1.254
!
```

Verification

Core#showipint brief
Vlan1 10.1.1.254 YES manual up up
Vlan10 10.1.10.254 YES manual up up
Vlan20 10.1.20.254 YES manual up up
Vlan30 10.1.30.254 YES manual up up
Vlan100 10.1.100.254 YES manual up up

Core#showip route
…
Gateway of last resort is not set

10.0.0.0/24 is subnetted, 5 subnets
C 10.1.1.0 is directly connected, Vlan1
C 10.1.10.0 is directly connected, Vlan10
C 10.1.20.0 is directly connected, Vlan20
C 10.1.30.0 is directly connected, Vlan30
C 10.1.100.0 is directly connected, Vlan100

Table 1

Note: if an SVI is down it needs to have a port configured to it you can check this with "show vlan" it must be in the vlan database to come up in show ipint brief

```
C:\>tracert 10.1.100.100

Tracing route to 10.1.100.100 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.1.10.254
  2   0 ms      0 ms      0 ms      10.1.100.100
```

Figure 2

Here from PC1 on Vlan 10 we can see in the trace route it reaches its default gateway on the core router before reaching Vlan 100.

```
C:\>tracert 10.1.100.100

Tracing route to 10.1.100.100 over a maximum of 30 hops:

  1   0 ms      1 ms      1 ms      10.1.30.254
  2   0 ms      0 ms      0 ms      10.1.100.100

Trace complete.
```

Figure 3

Same for PC3 on Vlan 30 reaching its default gateway 10.1.30.254 on the core router before reaching the server.

```
C:\>tracert 10.1.20.20

Tracing route to 10.1.20.20 over a maximum of 30 hops:

  1    0 ms        0 ms        0 ms        10.1.100.254
  2    *           0 ms        0 ms        10.1.20.20

Trace complete.

C:\>tracert 10.1.20.20

Tracing route to 10.1.20.20 over a maximum of 30 hops:

  1    1 ms        0 ms        0 ms        10.1.100.254
  2    0 ms        0 ms        0 ms        10.1.20.20

Trace complete.

C:\>
```

Figure 4

If you receive a * in the second ping don't panic retype and confirm. This is from the server to PC 2 it gets to its **default gateway on the core switch 10.1.100.254.**

VTP Theory

Vlan trunk protocol is used to propagate Vlans to multiple switches inside a domain to make configuration easier. Switches join the domain and learn the Vlans from the VTP server. By default switches are configured as a VTP server.

VTP packet inside 802.1Q frames

VTP protocol version: 1, 2, or 3

Vlan trunk protocol uses a client server model with three modes

1. **Server** – This is the default VTP mode that is used to modify the VLAN database and VTP configurations. VTP servers share their configurations to switches inside the VTP domain so synchronization can occur.

2. **Client** – VTP clients work the same way as VTP servers without the ability to change VLAN databases.

3. **Transparent** – VTP transparent switches are isolated by not advertising its configuration and not synchronising with any advertisements. They do forward VTP advertisements in VTP version 2.

VTP configuration

VTP Server config

1. Vtp mode server
2. Vtp domain ccna
3. Show vtp status

VTP Client Config //not required for real equipment a server can learn another servers Vlans

1. Vtp mode client
2. Vtp domain ccna
3. Show vtp status
4. Show vlan

Extra Examples and Resources

Cisco VTP

https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html