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 @DJninjaNZand 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 is as 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

These labs cover configuring access control lists which are essential in network security

Lab requirements

Configure the network as follows:

Lab 1: Basic config/VTP/Access ports

1. Restrict Router1 access using ACL 100
2. Inside PC1 can only access the HTTP server 1 using HTTP on subnet 10.1.1.0/24
3. Inside PC2 can only access the HTTP server 2 using HTTPS on subnet 10.1.1.0/24
4. No other PCs or servers on subnet 10.1.2.0/24 can access subnet 10.1.1.0/24 (Explicitly add this line. This is normally done to log the traffic with the word log, but PT does not support logging)
5. Hosts on subnet 10.1.2.0/24 can access any other network
6. Bind access list in the most efficient place on Router1

   Access1 = 10.1.1.1/24

   Access2 = 10.1.1.2/24

Access control lists / ACL

Used for creating a standard or extended list to filter packets based on defined rules for source and destination host IP addresses. These are then bound to interfaces facing in or out. ACL's help routers to discard traffic before it is sent all over the network being processed by multiple devices. ACL's are primarily configured on firewalls but can be configured on routers as well. The process of checking an ACL is it checks the first rules for matching statements either permit/deny. Once a match is found it will either forward or discard the traffic implicitly ACLs have deny all traffic at the end. Unfortunately packet tracer does not support some options. At the end of any ACL rule you can specify log on real equipment.

Standard ACL

- Standard Access lists 0-99 are configured far away from the source to prevent traffic being accidentally discarded
- Prioritize traffic by the source IP address
- This is the command syntax format of a standard ACL.
  access-list access-list-number {permit|deny} {host|sourcesource-wildcard|any}
- It must also be assigned under an interface directionallygoing out or coming in

Extended ACL

- Extended Access lists 100-199 these are configured close to the source because they are more specific and check a range of rules before discarding
- Filter based on Source / Destination IP address
- Filter based on TCP/UDP source/destination ports
- There is more ranges listed in iOS

Comparison between access lists

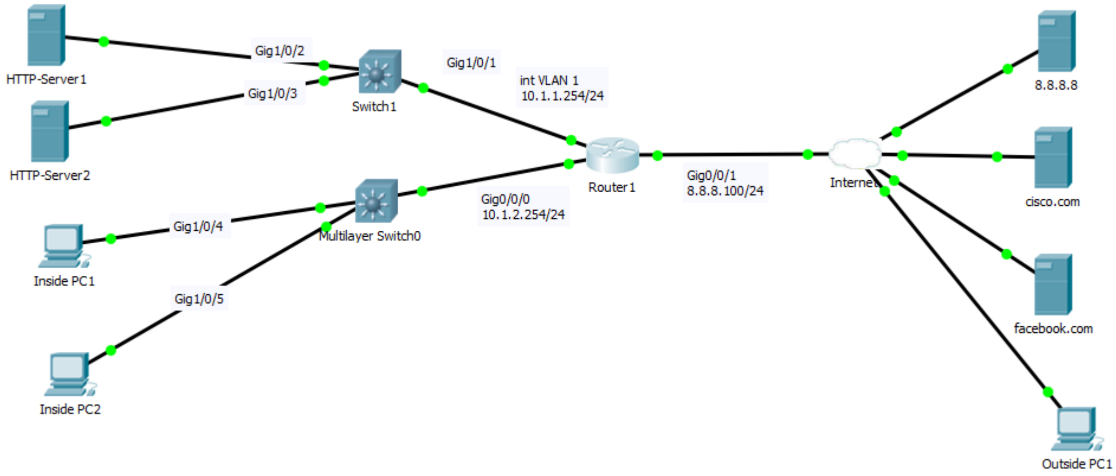
- ○ There are extended and standard ACLs
- ○ Location where they are placed
- ○ Number range
- ○ Keywords and options

Standard	**Extended**
Filters on **source address only**	Filters on **source and destination**
Permit or deny all IP/TCP	Specify **IP**, **protocol** and **port number**
Range 1-99 1300-1999	**Range** 100-199 2000-2699

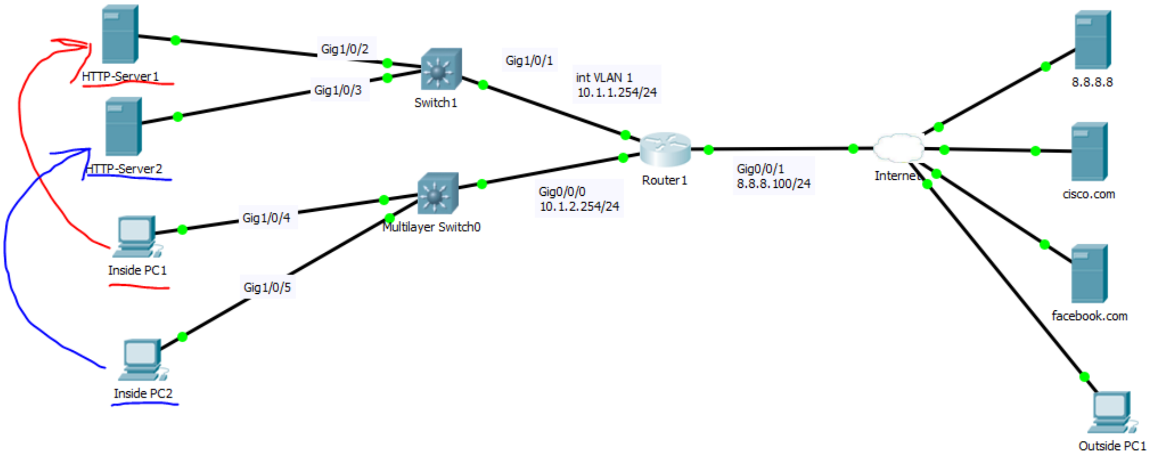
Well known port list

- 20: FTP data
- 21: FTP
- 22: SSH
- 23: Telnet
- 25: SMTP
- 49: Tacacs
- 69: TFTP
- 80: Http
- 88: Kerberos
- 161: SNMP
- 162: SNMP trap
- 179: BGP
- 443: HTTPS
- 4224 TCP: CDP

Lab 1 topology



Here we have a Router connected to two layer 3 switches and the internet showing an internal network and an external network. Potentially creating filters from the router to block internal or external traffic that matches conditions of source/destination IP or type of packet.



Make some diagrams about the problem and what we are doing for lab 1

Configurations and Verification

ACL lab 1
Router **Access List configuration** access-list 100 permit tcp host 10.1.2.101 host 10.1.1.100 eq80 access-list 100 permit tcp host 10.1.2.102 host 10.1.1.101 eq 443 access-list 100 deny ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list 100 permit ip 10.1.2.0 0.0.0.255 any **!** **Binding the access list to the correct port** interface GigabitEthernet0/0/0 ip address 10.1.2.254 255.255.255.0 ip access-group 100 in !
Verification **Router1#show access-lists** Extended IP access list 100 10 permit tcp host 10.1.2.101 host 10.1.1.100 eq www //converts port number 80 to word 20 permit tcp host 10.1.2.102 host 10.1.1.101 eq 443 30 deny ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255 40 permit ip 10.1.2.0 0.0.0.255 any **Ping and Web Browser** Ping 10.1.1.100 Ping 10.1.1.101 Ping cisco.com Ping facebook.com **From both inside PC's** **Web browser** 10.1.1.100 https://10.1.1.101 facebook.com cisco.com **Router1#show access-lists //we can see traffic has been generated** Extended IP access list 100 10 permit tcp host 10.1.2.101 host 10.1.1.100 eq www (31 match(es)) 20 permit tcp host 10.1.2.102 host 10.1.1.101 eq 443 (6 match(es)) 30 deny ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255 (533 match(es)) 40 permit ip 10.1.2.0 0.0.0.255 any (351 match(es))

Table 1

Note1:Access list logging can be CPU intensive on real hardware and negatively affect the network device. You can configure logging intervals on real hardware along with rate and buffer limits

ip access-list logging interval 10

Note 2: Bind the port to the most efficient port with

Note 3: Port 80 is http 443 is httpss

Note 4: Editing ACLs

Router1(config)#ip access-list extended 100 to enter the access list you can delete specific lines

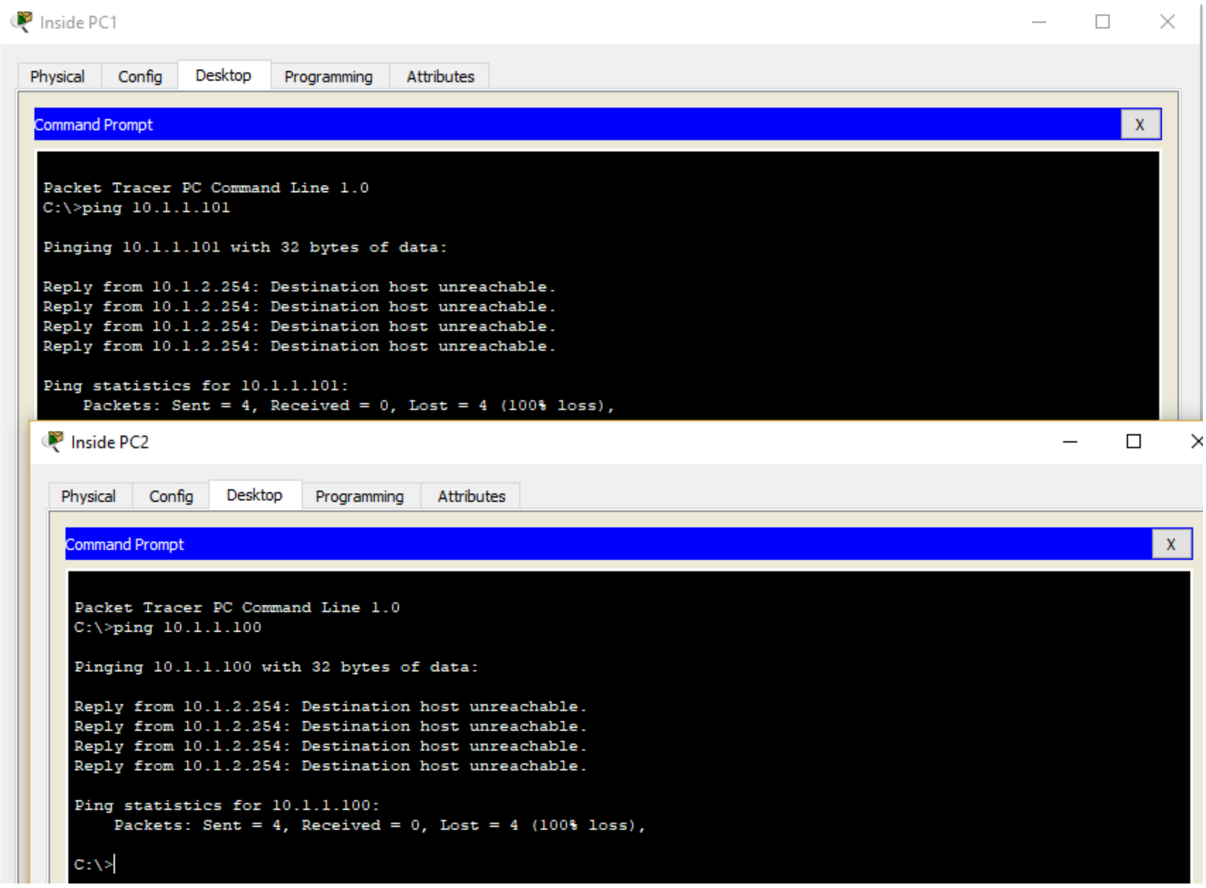
no20

You can read the entry with #**20 permit tcp host 10.1.2.102 host 10.1.1.101 eq 443**

Note 5: Before ACL apply in the real world router1#reload in 10

In case you are locked out because of a misconfigured ACL

Verification



```
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.101

Pinging 10.1.1.101 with 32 bytes of data:

Reply from 10.1.2.254: Destination host unreachable.
Reply from 10.1.2.254: Destination host unreachable.
Reply from 10.1.2.254: Destination host unreachable.
Reply from 10.1.2.254: Destination host unreachable.

Ping statistics for 10.1.1.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

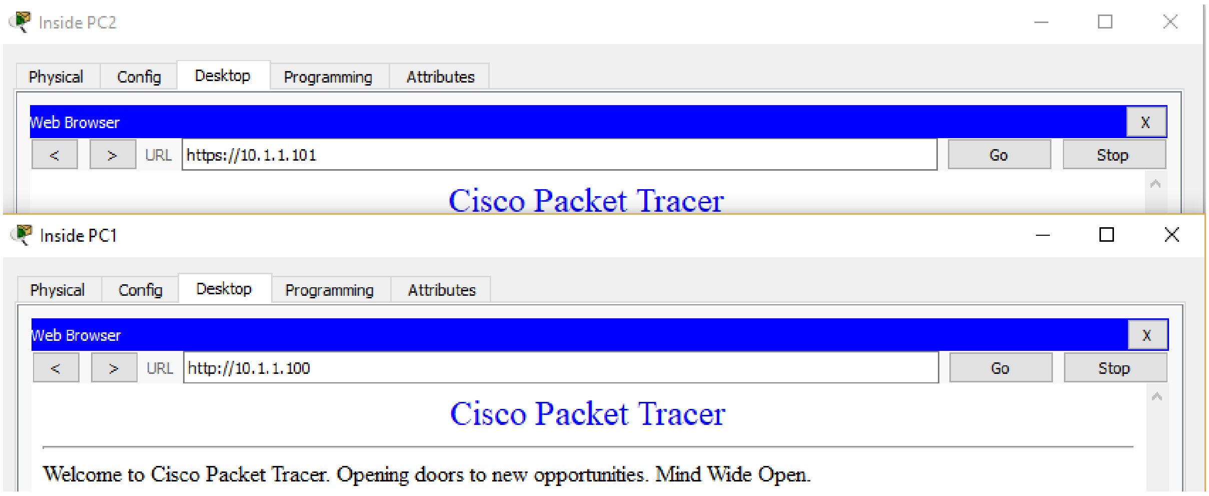
```
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.100

Pinging 10.1.1.100 with 32 bytes of data:

Reply from 10.1.2.254: Destination host unreachable.
Reply from 10.1.2.254: Destination host unreachable.
Reply from 10.1.2.254: Destination host unreachable.
Reply from 10.1.2.254: Destination host unreachable.

Ping statistics for 10.1.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



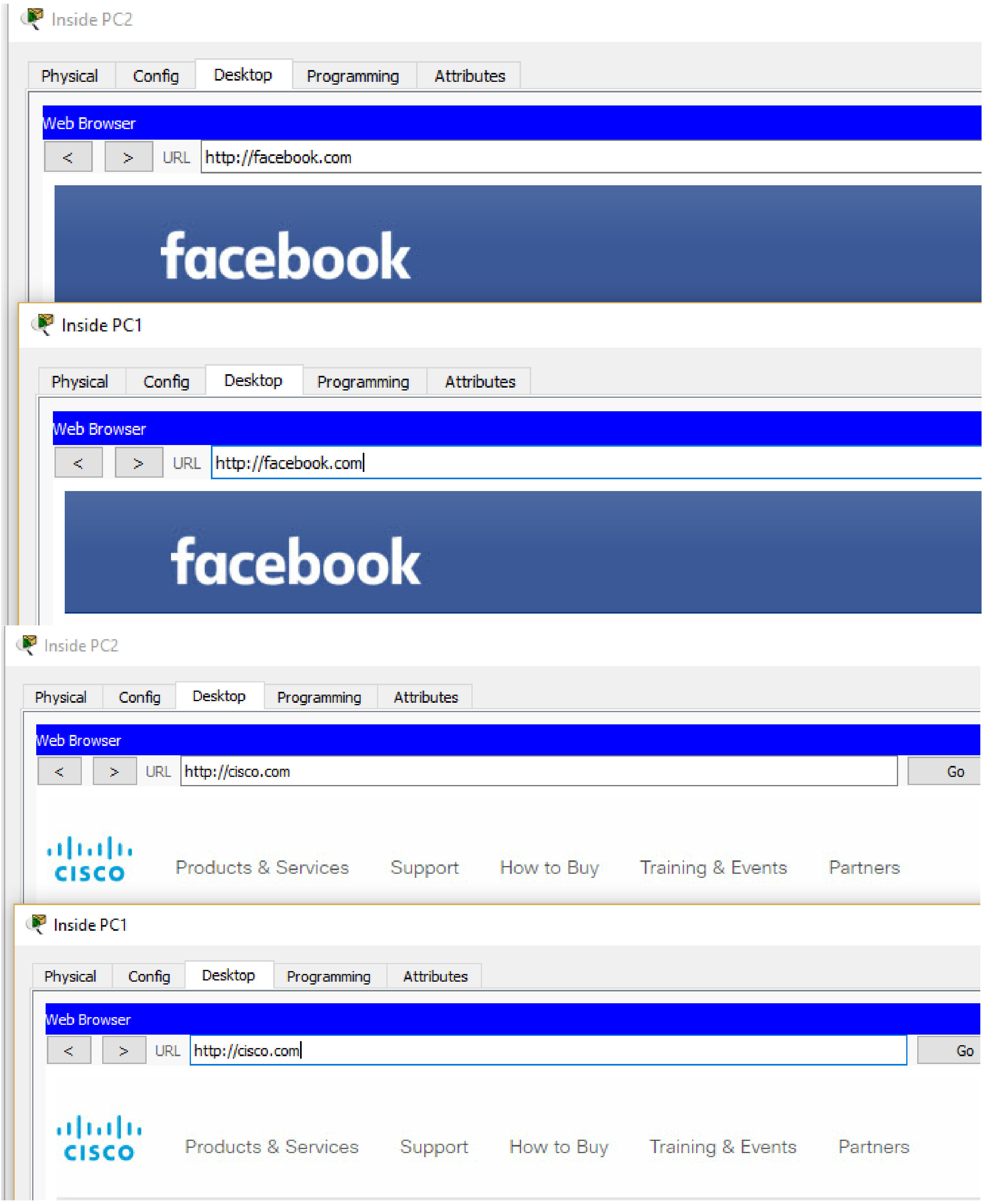
URL: https://10.1.1.101

Cisco Packet Tracer

URL: http://10.1.1.100

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.



Inside PC2

URL http://facebook.com

Inside PC1

URL http://facebook.com

Inside PC2

URL http://cisco.com

Inside PC1

URL http://cisco.com

Extra Examples and Resources

IP Access Lists – Cisco https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

Common ACLS – Cisco https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vacl.pdf

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 @DJninjaNZand 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 theauthors nor Network Experts Internet Ltd, assume any liability or responsibility to any person or entity withrespect 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 aforementionedauthors. Any similarities between material presented in these notes and the actual CCNA exam material iscompletely 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.