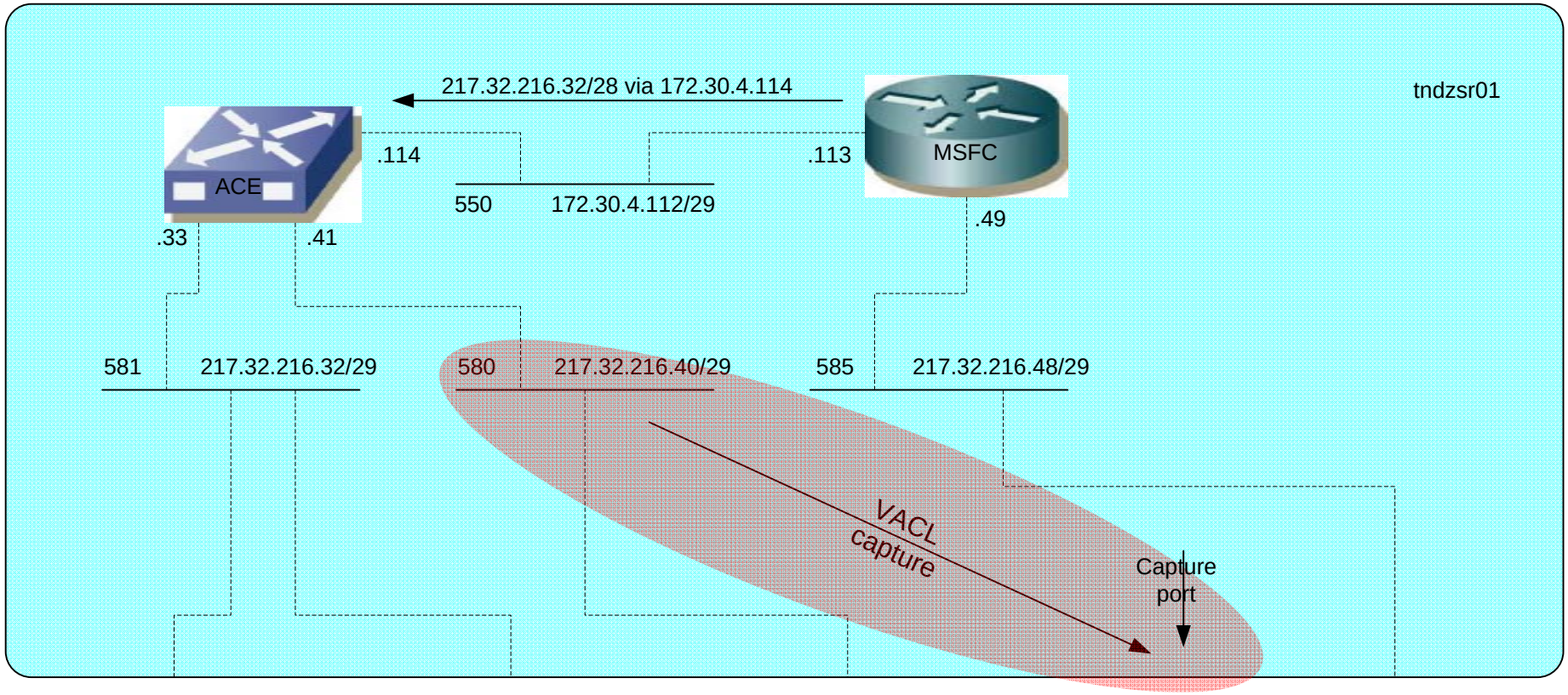

Using VLAN ACL (VACL) to capture traffic requires 4 basic steps:

1) define ACLs to match traffic of interest

2) create a VLAN access-map (or more than one) to use these ACLs to match traffic and then perform actions upon it

3) apply the access-map(s) to the VLAN(s) from which traffic is to be captured.

4) enable ‘capture’ on the capture interface for the VLAN(s) of interest.

ACLs can be any of standard or extended MAC or IP ACLs (or a mix) to select traffic based on any combination of layer-2 to layer-4 properties.

The first example below is a named, extended IP access-list that matches any IP traffic coming from the lab /28 subnet to any destination.

The second example below matches any IP traffic. The need for this will be seen in the sections on access-maps

```
ip access-list extended lab-source
 permit ip 81.142.247.64 0.0.0.15 any

ip access-list extended aa
 permit ip any any
```

Access-maps are constructed much like route-maps, with one or more ‘statements’, each containing a ‘match’ clause and an ‘action’ clause. The ‘action’ clause can take 3 keywords – ‘drop’, ‘forward’ or ‘redirect’, Drop and Forward can then be followed by other (optional) keywords – ‘log’ or ‘capture’: Redirect is followed by an interface name.
For the purposes of traffic capture, we will look specifically at the ‘forward [capture]’ keywords:
Refer to the example below.

1 This line defines statement 10 of an access-map called ‘test4’

```
1   vlan access-map test4 10
2    match ip address cw lab-source
3    action forward capture
4   vlan access-map test4 20
5    match ip address aa
6    action forward
```

2 This line says, match traffic using IP access-lists ‘cw’ and ‘lab-source’: These are logically ORed. This shows that it is possible to define what you want to match either in a single ACL with one or more lines, OR in multiple ACLs (if perhaps it makes more sense to keep certain ranges/ ports grouped together) and then refer to a set of ACLs in a single ‘match’ clause.

```
1   vlan access-map test4 10
2    match ip address cw lab-source
3    action forward capture
4   vlan access-map test4 20
5    match ip address aa
6    action forward
```

3 having matched traffic according to the ACL(s) used in line 2, this line then says what to do with it. In this case we want to forward the traffic (as the switch would normally do anyway) AND capture it.

NOTE: access-maps have an implict ‘deny any’ (like ACLs) so in this case, since statement 10 is matching only a subset of all traffic that will potentially cross the VLAN that this is applied to there MUST be a second statement that matches all other traffic and forwards it (if this is what you want to happen!) otherwise it will be dropped.

```
1   vlan access-map test4 10
2    match ip address cw lab-source
3    action forward capture
4   vlan access-map test4 20
5    match ip address aa
6    action forward
```

4 A second statement of the access-map (numbered 20 in this case) is necessary here to catch all other traffic NOT matched by statement 10, otherwise it would be dropped.

```
1   vlan access-map test4 10
2    match ip address cw lab-source
3    action forward capture
4   vlan access-map test4 20
5    match ip address aa
6    action forward
```

5 match all traffic not already matched by the ACLs used in statement 10 against an ACL called ‘aa’, which matches anything.

```
1   vlan access-map test4 10
2    match ip address cw lab-source
3    action forward capture
4   vlan access-map test4 20
5    match ip address aa
6    action forward
```

6 forward all other traffic. That is, switch it as it would have been switched anyway.

Since the match clause in line 2 can utilise multiple ACLs, each of which can contain multiple ‘permit’ statements there should usually be no need for more than 2 access-map statements.

```
1   vlan access-map test4 10
2    match ip address cw lab-source
3    action forward capture
4   vlan access-map test4 20
5    match ip address aa
6    action forward
```

The VLAN filter is used to apply the access-map to a VLAN. Once this is done filtering has started.

The same access-map can be applied to multiple VLANs, but each VLAN can have only one access-map applied at a time.

If the map is to be applied to multiple VLANs they can be specified as a comma-separated list, or if the VLAN numbers are contiguous as X-Y (see below for examples).

NOTE: If using the comma-separated format, there must be whitespace after the commas.

```
vlan filter test4 vlan-list 580
Or
vlan filter test4 vlan-list 580, 581, 582 etc…
Or
vlan filter test4 vlan-list 580-582
```

The last task to perform is to enable capture on the interface out of which you want the captured frames to be sent. This is done by using options of the “switchport” command.

1 specify the interface

NOTE
The capture interface CANNOT be a PortChannel interface.

```
1   Interface x/y
2    switchport
3    switchport mode {access | trunk}
4    switchport capture
5    switchport capture allowed vlan 580
Or
5    switchport capture allowed vlan 580,581,582 etc..
Or
5    switchport capture allowed vlan 580-582
```

2 Configure the interface as a switchport. This is mandatory – VACL cannot use interfaces configured as layer-3

```
1   Interface x/y
2    switchport
3    switchport mode {access | trunk}
4    switchport capture
5    switchport capture allowed vlan 580
Or
5    switchport capture allowed vlan 580,581,582 etc..
Or
5    switchport capture allowed vlan 580-582
```

3 Configure the mode of the capture interface: Access or Trunk

The capture interface can be either an access interface or a trunk. In the first case frames are sent without a VLAN tag, regardless of which VLAN they were captured from. In the second case frames are sent with the VLAN tag of the VLAN they were captured from.

```
1   Interface x/y
2    switchport
3    switchport mode {access | trunk}
4    switchport capture
5    switchport capture allowed vlan 580
Or
5    switchport capture allowed vlan 580,581,582 etc..
Or
5    switchport capture allowed vlan 580-582
```

4 Enable capture on the interface.

This prepares the interface for capturing frames but DOES NOT start the actual capture yet.

```
1   Interface x/y
2    switchport
3    switchport mode {access | trunk}
4    switchport capture
5    switchport capture allowed vlan 580
Or
5    switchport capture allowed vlan 580,581,582 etc..
Or
5    switchport capture allowed vlan 580-582
```

5 Specify which traffic is to be captured by listing the VLAN(s) it is to be captured from.

This can be specified in a few ways: Either as a single VLAN number, or a comma-separated list, or as a hyphen-separated range.

NOTE: If using the comma-separated format there must be NO whitespace between the values and the commas!

NOTE: It is possible to list any VLAN (even non-existent ones). If a VLAN filter is not running on one (or more) of those VLANs at the time, no traffic will be captured from them.

```
1   Interface x/y
2    switchport
3    switchport mode {access | trunk}
4    switchport capture
5    switchport capture allowed vlan 580
Or
5    switchport capture allowed vlan 580,581,582 etc..
Or
5    switchport capture allowed vlan 580-582
```