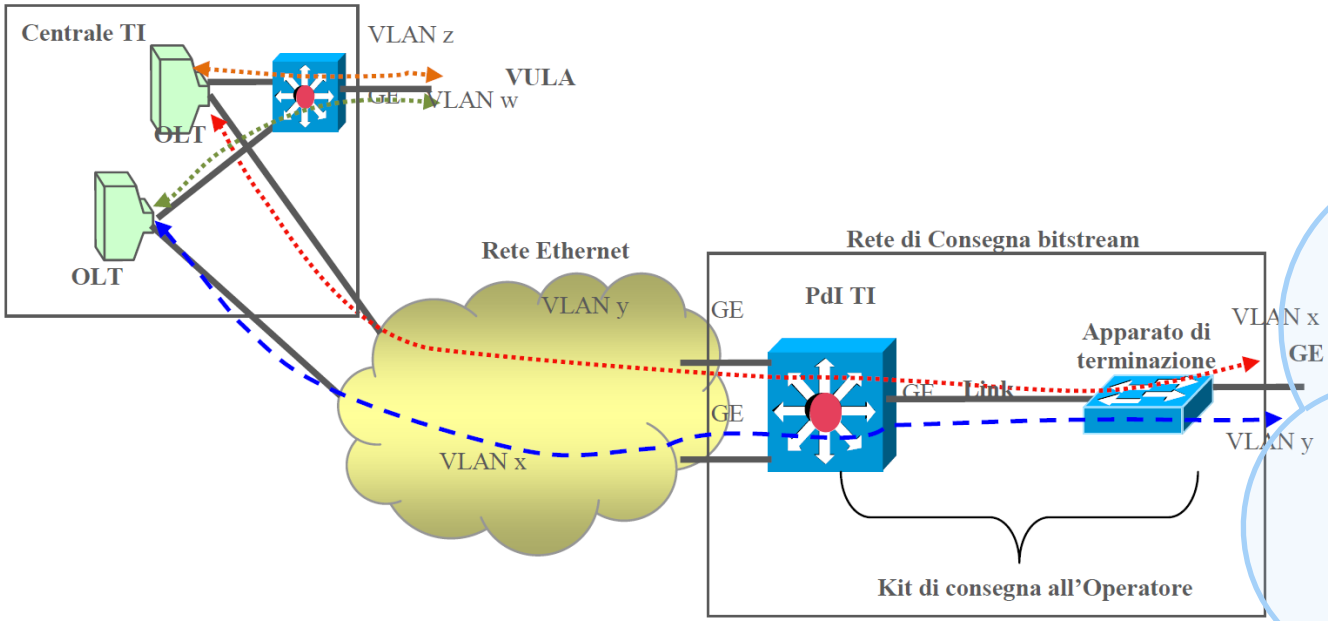
Radius with IOS XE andXR

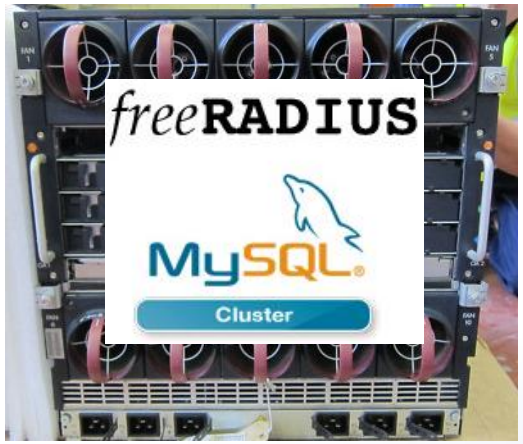
TWT

CONNECT YOUR BUSINESS

The Italian Model of Bitstream



IOS XE and XR



Radius AAA

TWT
CONNECT YOUR BUSINESS

Radius attributes some the same

Framed-Protocol	=	PPP
Framed-IP-Netmask	=	255.255.255.255
Framed-MTU	=	1500
Service-Type	=	Framed-User
Framed-IP-Address	=	192.0.2.1
Framed-ipv6-prefix	=	2001:DB8::0/64
Framed-Interface-Id	=	0:0:0:1
cisco-avpair	+=	ip:sub-qos-policy-out=MyPolicy
Framed-IPv6-Route	+=	2001:DB8:ABCD::0/64 2001:DB8::01 1
Framed-Route	+=	192.0.2.224 255.255.255.252

TWT
CONNECT YOUR BUSINESS

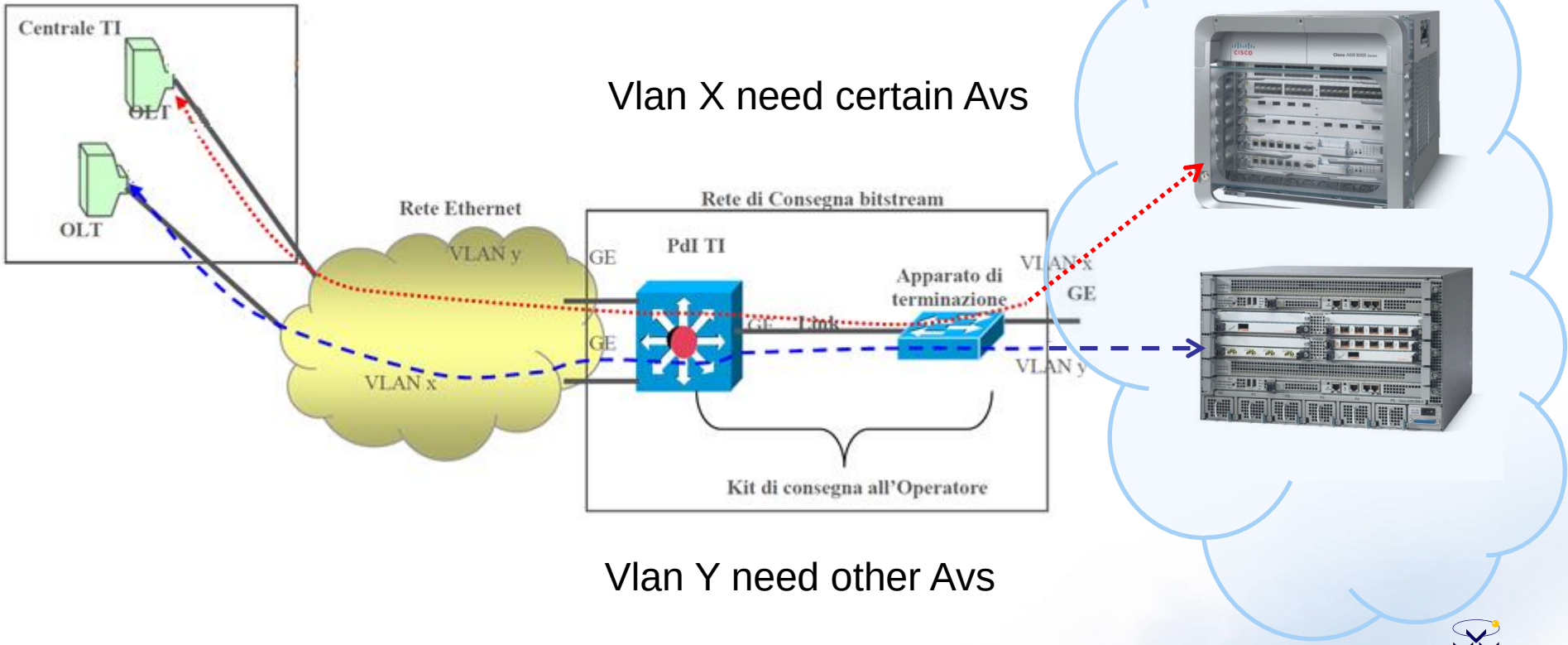
Radius Attributes some are not

IOS XE	IOS XR
cisco-avpair += ip:ip-unnumbered=loopback 0	cisco-avpair += ipv4:ipv4-unnumbered=loopback 0
cisco-avpair += ip:outacl#1=deny udp any any eq 53 cisco-avpair += ip:outacl#2=permit ip any any	cisco-avpair += "ipv4:outacl=ACL-NAME"
Nothing Needed for outbound L2TP	Service-Type = Outbound-User

TWT
CONNECT YOUR BUSINESS

Results

IOS XE and XR



Vlan X need certain Avs

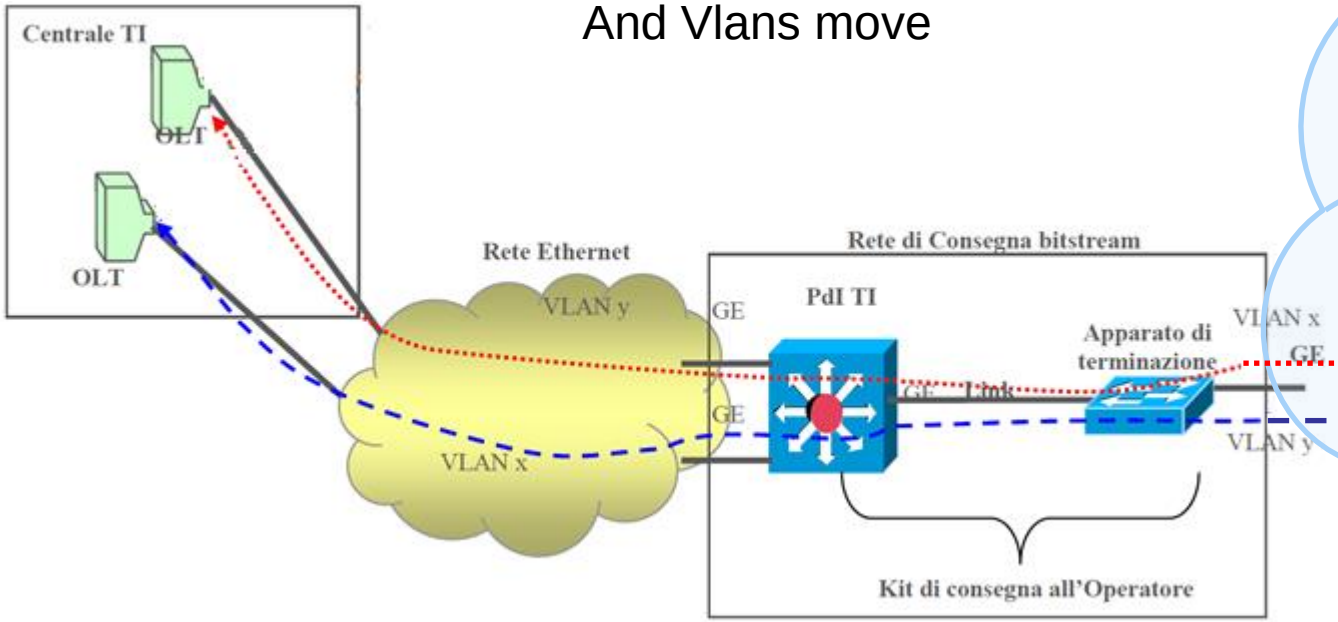
Vlan Y need other Avs

TWT
CONNECT YOUR BUSINESS

Problem

IOS XE and XR

Networks are ever changing
And Vlans move



TWT
CONNECT YOUR BUSINESS

What to do?

- What happens if we pass both parameter?

IOS XE Ignores unsupported AVs and Authenticates

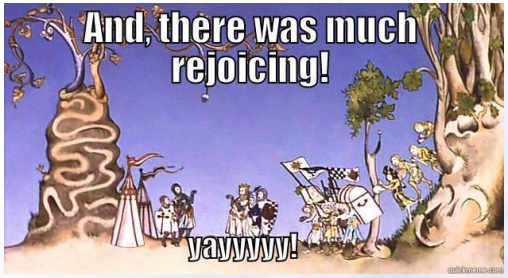
IOS XR does not . Session remains down

- Can the routers support the same AVs?

NO.

- Can we send different parameters based on nas ip address?

YES



TWT
CONNECT YOUR BUSINESS

Our Solution

Create different radius reply tables for each IOS

Modify sql.conf to use tables

```
sql sql1
        database  = "mysql"
        radius_db = "radius"

        acct_table1      = "radacct"
        authcheck_table  = "radcheck"
        authreply_table  = "radreply"
        groupcheck_table = "radgroupcheck"
        groupreply_table = "radgroupreply"
        usergroup_table  = "radusergroup"

sql sqlNew1
        database  = "mysql"
        radius_db = "radius"

        acct_table1      = "radacct"
        authcheck_table  = "radcheck"
        authreply_table  = "radreply2"
        groupcheck_table = "radgroupcheck"
        groupreply_table = "radgroupreply2"
```

And 2 new virtual modules in radiusd.conf

```
    redundant redundant_sql {
        sql1
        sql2
}

redundant redundant_sqlNew {
        sqlNew1
        sqlNew2
}
```

TWT
CONNECT YOUR BUSINESS

Our Solution 2

Reply from correct tables for each nas ip address

```
if (Realm == 'DEFAULT' || Realm == 'NULL' || Realm == 'LOCAL' ) {
        if (NAS-IP-Address =~ /^(192\.0\.2\.1|192\.0\.2\.2)$/ ) {
                redundant_sqlNew
        }
        else {
                redundant_sql
        }
}
```

TWT
CONNECT YOUR BUSINESS

Advantages

- Dynamic – Attributes returned change automatically depending on source
- One Database to rule them all
- Same user/group check tables
- All accounting in same place
- Easy to integrate into portals/systems