

# TACACS+



AfNOG 2012 AR-E Workshop

# User Authentication

---

- ❑ Common username and password
  - **DO NOT!!**
- ❑ Usernames and passwords on router:
  - Does not scale
  - New user - have to go around whole network to add username password
  - Change password - have to go around whole network to change password
  - User leaves - have to go around whole network to remove password and change enable secret

# User Authentication

---

- Best solution: centralised authentication system
  - And that is TACACS+
  - Supported on all Cisco routers and several other makes too
  - Requires TACACS+ software running on a Unix type system
  - Get it from [www.shrubbery.net/tac\\_plus/](http://www.shrubbery.net/tac_plus/) and build/compile it yourself (simple)

# Configuration on Cisco IOS

---

```
aaa new-model
```

```
!
```

```
aaa authentication login default group tacacs+ enable
```

```
aaa authentication enable default group tacacs+ enable
```

```
!
```

```
aaa authorization commands 0 default group tacacs+ none
```

```
!
```

```
aaa accounting exec default start-stop group tacacs+
```

```
aaa accounting commands 15 default start-stop group tacacs+
```

If doing command authorisation



If doing command accounting



If checking each time configure mode is entered



# Configuration on Cisco IOS

---

```
enable secret bkup5crt
```

← Only used if TACACS+ server fails

```
!
```

```
ip tacacs source-interface Loopback0
```

```
!
```

```
tacacs-server host 215.17.1.1
```

```
tacacs-server host 215.17.5.35
```

```
tacacs-server key t4cpk3y
```

← Authentication key with server

```
!
```

```
access-list 3 permit 215.17.1.0 0.0.0.15
```

```
access-list 3 deny any log
```

```
!
```

```
line vty 0 4
```

```
  access-class 3 in
```

```
  transport input ssh
```

```
  transport preferred none
```

```
!
```

# Unix configuration file (part1)

---

## □ /usr/local/etc/tac\_plus.cfg

```
key = "t4cpk3y"
##### User Definitions #####
user = $enab15$ {
    login = des #####
    name = "Enable User"
    member = admin
}
user = philip {
    login = des #####
    member = admin
    name = "Philip Smith"
}
```

Enable Password here!




User has unique password




## /usr/local/etc/tac\_plus.cfg (2)

---

```
user = john {
    member = staff
    name = "John Smith"
}
user = bill {
    member = noc
    name = "Bill Jones"
}
##### Group Definitions #####
group = admin {
    default service = permit
}
```

 **User has shared staff password**

 **User has shared NOC password**

## /usr/local/etc/tac\_plus.cfg (3)

---

```
group = staff {
    default service = permit
    cmd = enable {
        deny .*
    }
    login = des #####
}
group = noc {
    # group noc is a member of staff
    default service = permit
    login = des #####
}
```



# Setting DES password

---

- ❑ Unix server install has the `/usr/local/bin/tac_passwd` command
- ❑ To create password:
  - Ask user to run above command
  - Then insert into the resultant DES key into server configuration file
  - Restart TACACS+ server