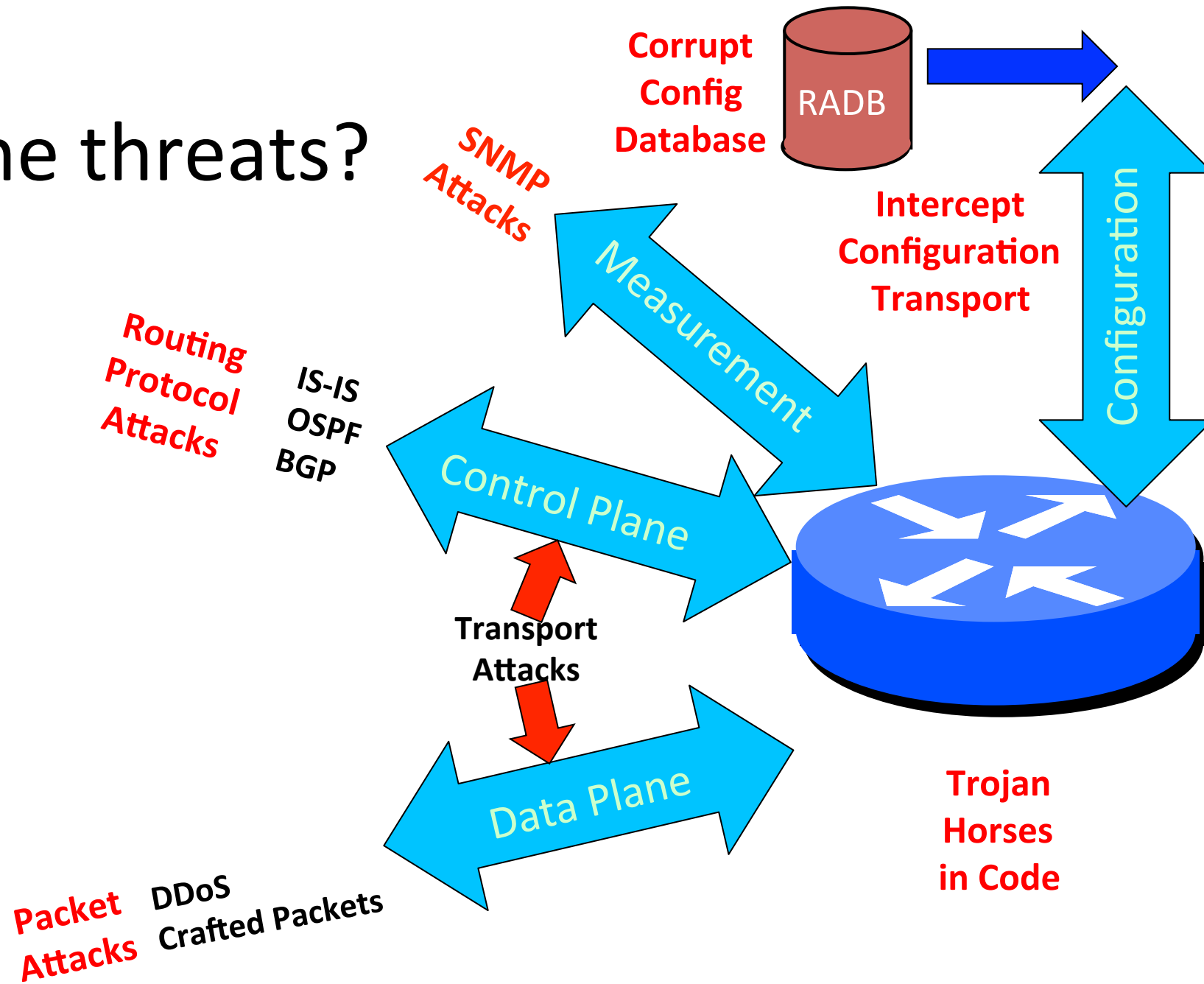
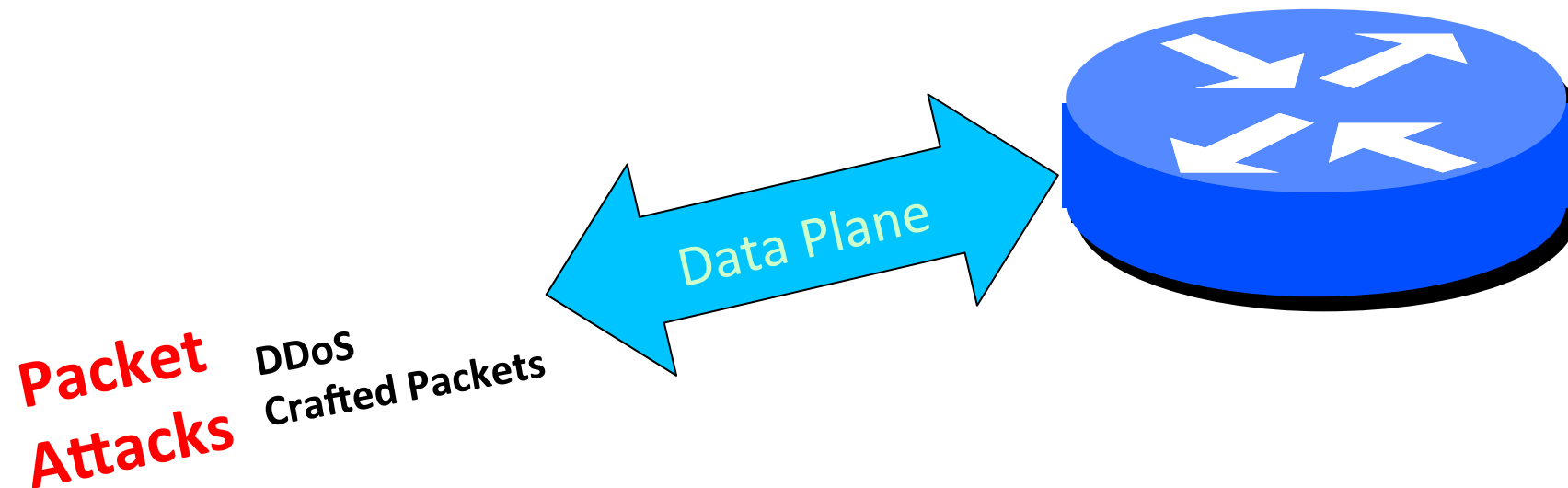


Protecting Network Infrastructure - Routers, Switches, etc.

What are the threats?



- DDoS is Continuous in Large Networks
- Mitigation Techniques such as Black Hole but as the last resort
- Filter & Patch is all you can do



ACL- Access Control Lists

NTP ACL

SNMP ACL

VTY ACL

Try using NAMED Access Control List –
makes the work of a Network Admin
easier

NTP ACLs

```
! Core NTP configuration
ntp server 209.20.186.192           ! ntp.psg.com
ntp server 147.28.0.36             ! rip.psg.com
ntp server 147.28.0.62             ! psg.com
!
ntp source Loopback0
!
access-list 46 remark utility ACL to block everything
access-list 46 deny any
!
access-list 47 remark NTP peers/servers we sync to/with
access-list 47 permit 209.20.186.192
access-list 47 permit 147.28.0.36
access-list 47 permit 147.28.0.62
access-list 47 deny any
!
! NTP access control
ntp access-group query-only 46     ! deny all NTP control queries
ntp access-group serve 46          ! deny all NTP by default
ntp access-group peer 47           ! permit sync to peer(s)/server(s)
ntp access-group serve-only 46     ! deny NTP time sync requests
ntp authenticate                   ! enable NTP authentication
ntp authentication-key [key-id] md5 [hash] ! define a NTP authentication key
```

- Routing was Designed With no Concern for Security
- Attacks can be Close or Remote, e.g. YouTube Incident

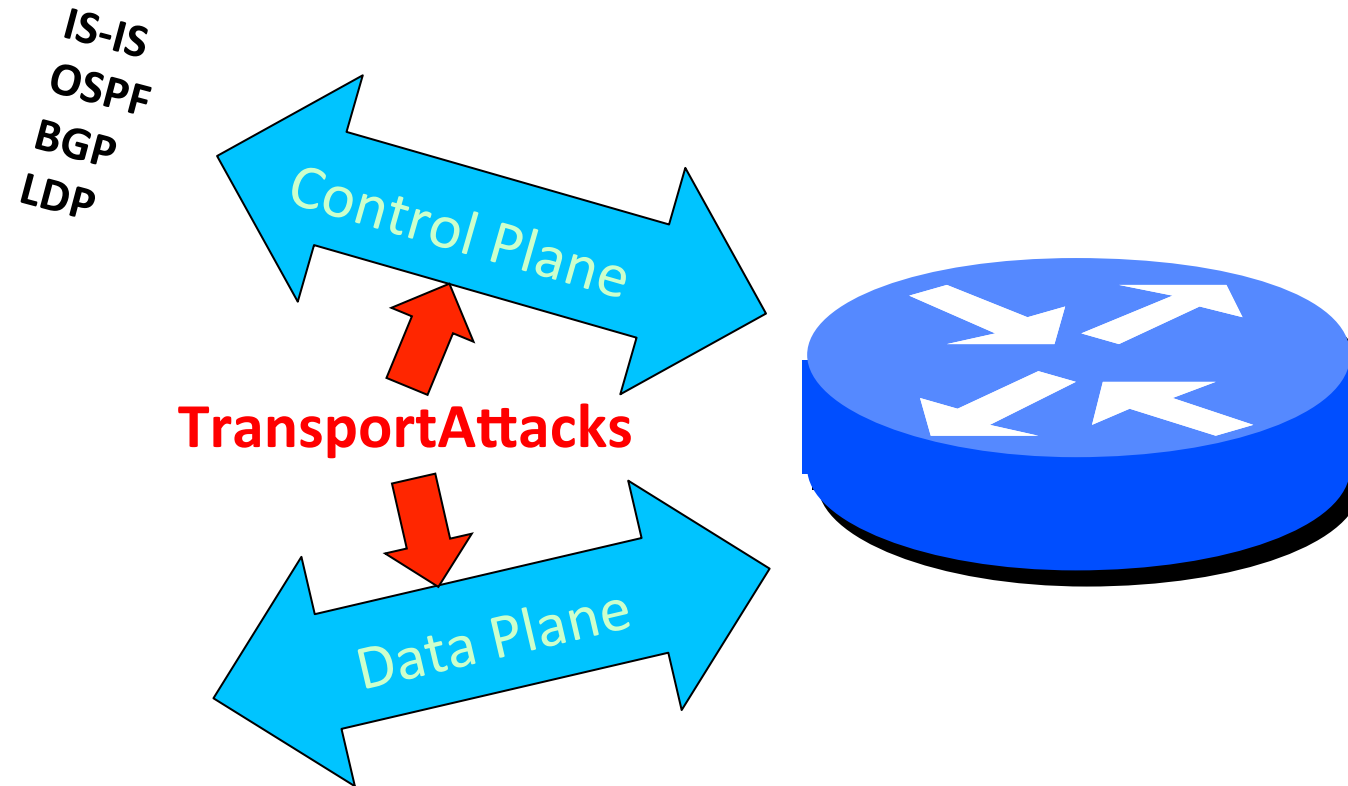
**Routing
Protocol
Attacks**

IS-IS
OSPF
BGP
LDP



- IS-IS a bit Less Vulnerable as it is not Over IP, it is CLNP
- Use MD5 Auth for Authentication
- Other Protections Very Active in IETF

- Assume Monkeys are in the Middle
- Authenticate all Control Traffic, MD5 or Stronger
- Teach Customers to Encrypt: https, imaps, ssh, ...
- WPA2 (enterprise) on WiFi



MD5 Authentication

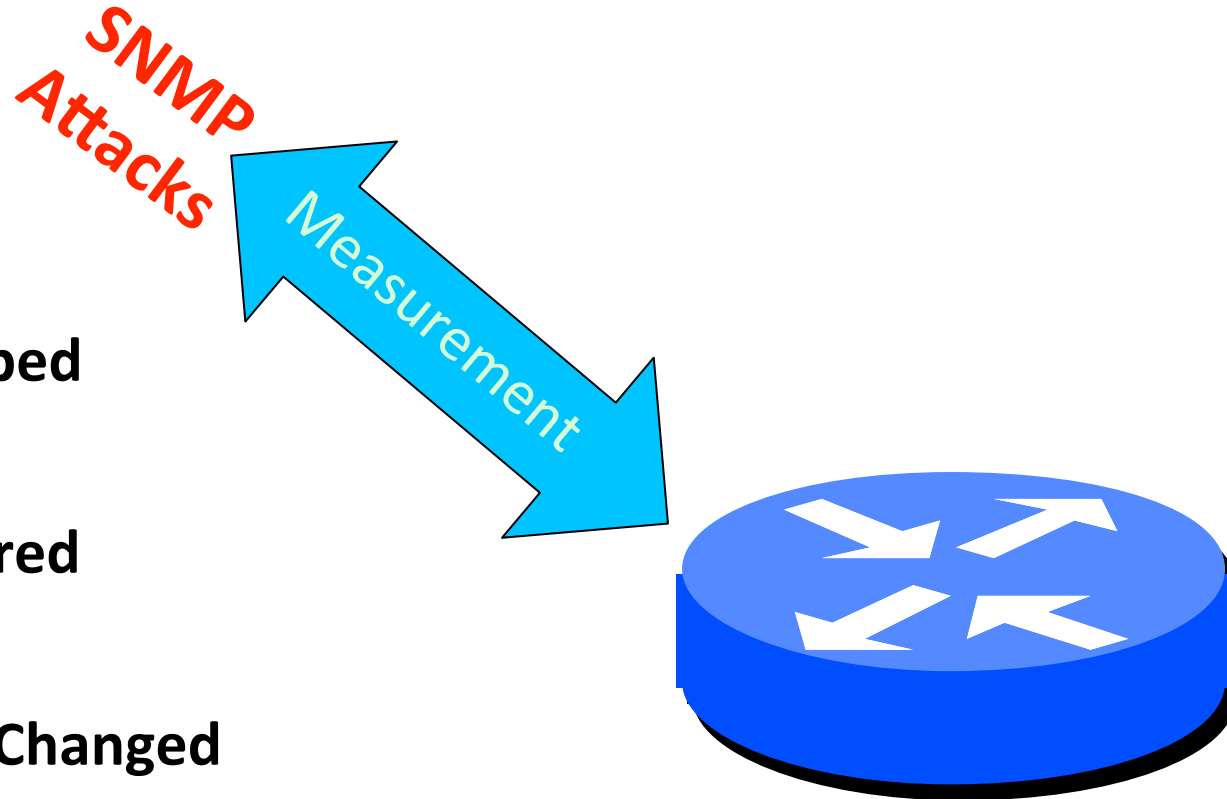
- neighbor 199.238.113.9 remote-as 2914
- neighbor 199.238.113.9 description
variuo customer aggregation
- neighbor 199.238.113.9 password 7
0117575757581E172045

Protects against MITM resets Fake Peers

IS-IS

- Is Layer-2, CLNP, not Layer-3
- So Can Not be Attacked Remotely
- Has Other Advantages over OSPF, such as Scaling to 1,000 routers
- Most Larger Providers Run IS-IS

- Occasional New Ones
- Usually against ASN.1
- Network may be Mapped
- Traffic may be Monitored
- Configuration may be Changed
- Use ACLs on What Host may SNMP
- Defense is Using SNMPv3 which is Encrypted



Simple SNMP Precaution

```
! snmp pollers
```

```
Ip access-list standard v4snmp-access
```

```
permit host 129.250.32.1
```

```
Deny ip any any
```

```
snmp-server enable (for all traps)
```

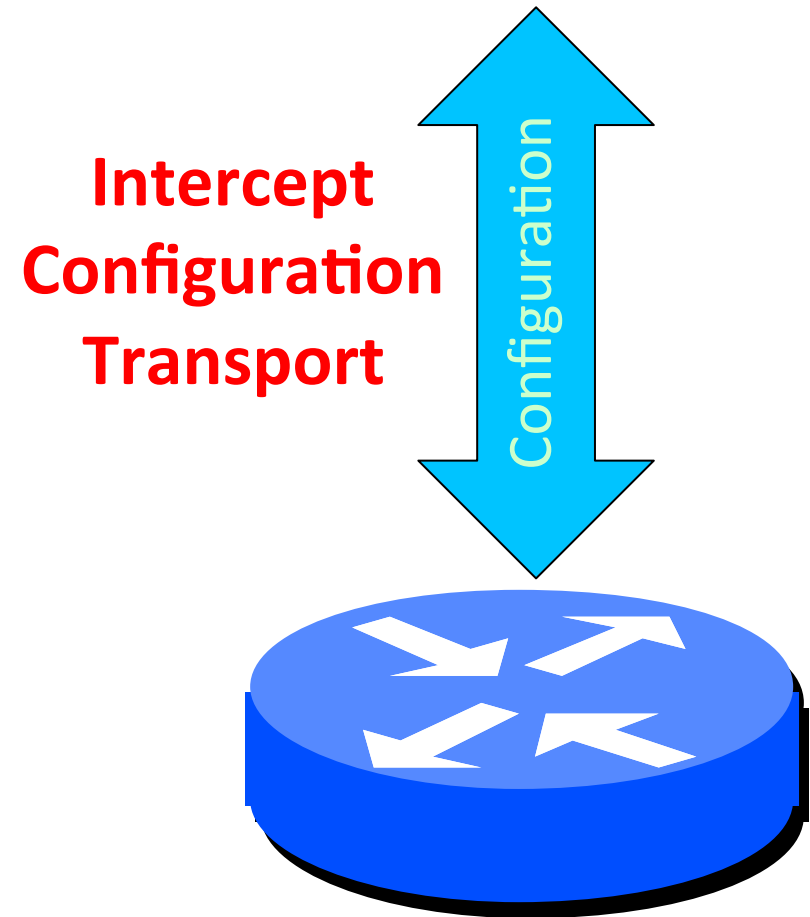
```
snmp-server enable traps bgp
```

```
snmp-server enable traps config
```


```
snmp-server enable traps envmon
```

```
snmp-server community <secret> R0 v4snmp-access
```

- **Tapping Configuration Session**
 - **Stealing Password**
 - **Stealing Configuration**
- **DO NOT USE Telnet**
- **Configure Over ssh**
- **Restrict ssh to Special Hosts**



ssh Access Control List

- `line vty 0 4`
 - `secret 5 071C205F4600140C5C`
 - `exec-timeout 0 0`
 - `transport input ssh`
 - `access-class vty4 in`
 - `ipv6 access-class vty6 in`
 - `transport preferred none`
 - `ip access-list standard vty4`
 - `permit 147.28.0.0 0.0.7.255`
 - `permit 198.180.150.0 0.0.0.255`
 - `permit 198.180.152.0 0.0.0.255`
 - `!`
 - `ipv6 access-list vty6`
 - `permit ipv6 2001:418:1::/48 any`
- 

Cisco password 'encryption' is trivial to attack
So protect your configurations!

Creative Commons: Attribution-NonCommercial-ShareAlike

SSH Access list with TACACS Server

Possibly use a TACACS Server for centralized login to the data comm devices.

AAA- Authorization,
Authentication and accounting
Create multiple user with different
user privilege

- `ip access-list standard v4vty-access`
- `Permit ip 192.168.1.1 0.0.0.7`
- `Deny any log (log is optional)`
- `line vty 0 4`
- `exec-timeout 0 0`
- `transport input ssh`
- `access-class v4vty-access in`
- `transport preferred none`

192.168.1.1 0.0.0.7

