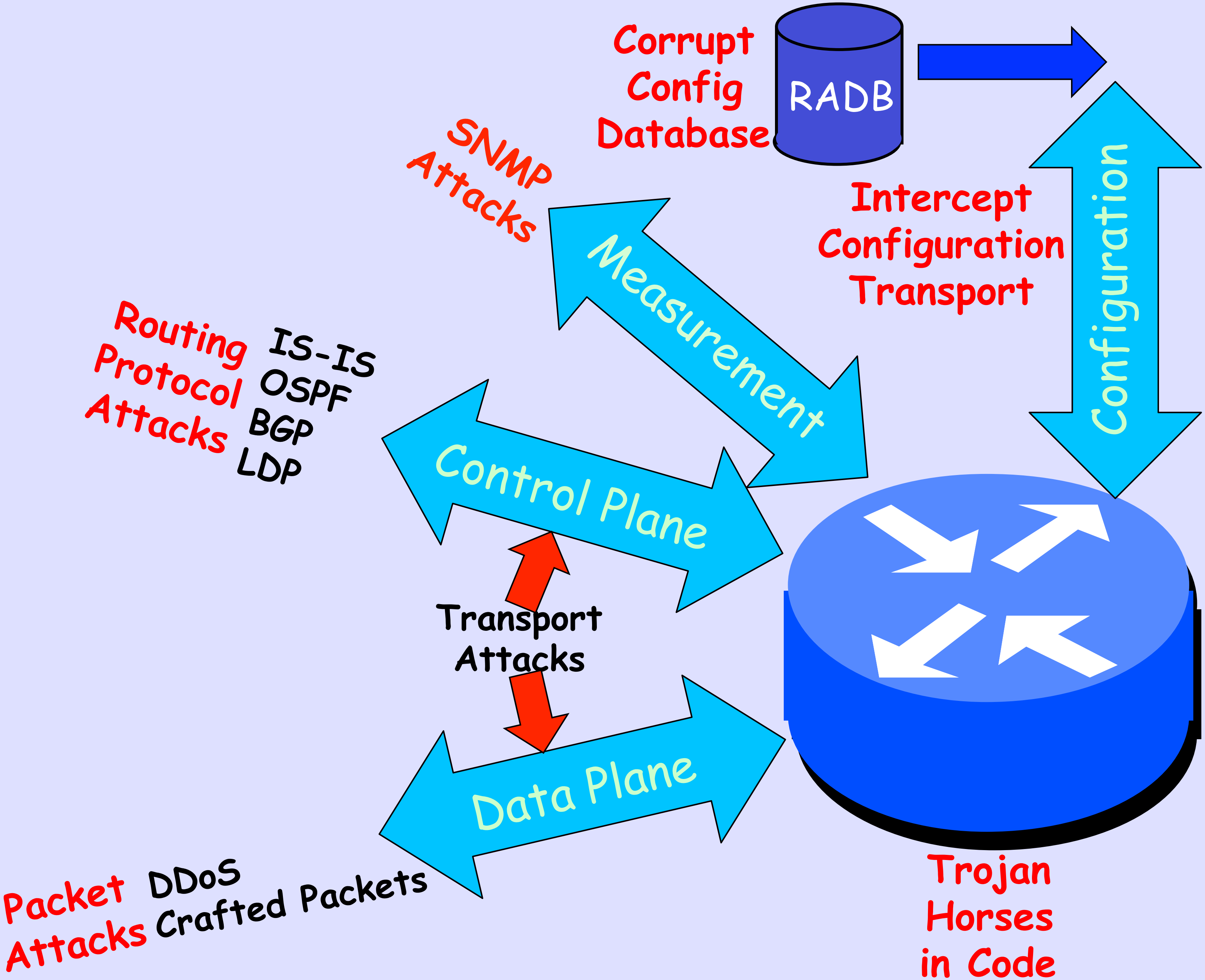
2-3-1
Protecting
Network Infrastructure
Routers, Switches, etc.



Corrupt
Config
Database

SNMP
Attacks

Intercept
Configuration
Transport

Routing
Protocol
Attacks

IS-IS
OSPF
BGP
LDP

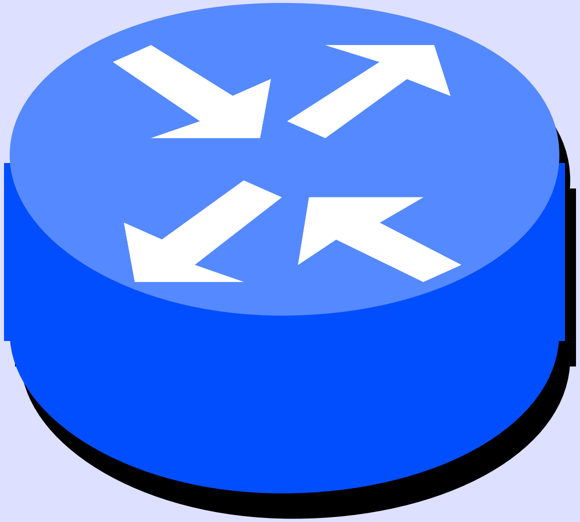
Transport
Attacks

Packet
Attacks

DDoS
Crafted Packets

Trojan
Horses
in Code

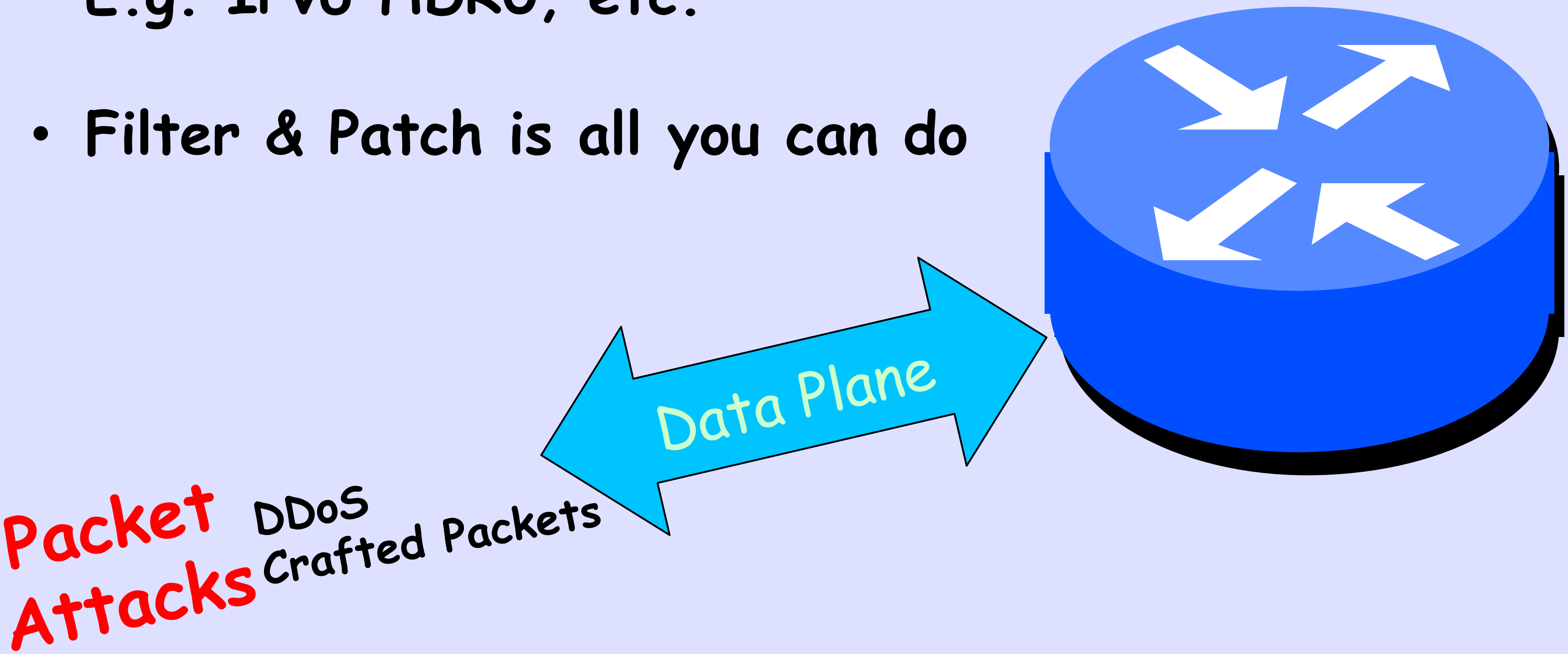
- Could Spy on Protocols, Data, or Configuration
- Could Alter Protocols, Data, or Configuration
- Would Require Vendor Collusion
- Nation State Attack
- Considered Unlikely
- Only Protection is Code Audit



Trojan Horses in Code

- DDoS is Continual Every Day in Large Networks
- Mitigation Techniques such as Black Hole
- Crafted Packets Exploit Weakness in Vendor Code

  E.g. IPv6 HDR0, etc.
- Filter & Patch is all you can do



Data Plane

Packet Attacks

DDoS

Crafted Packets

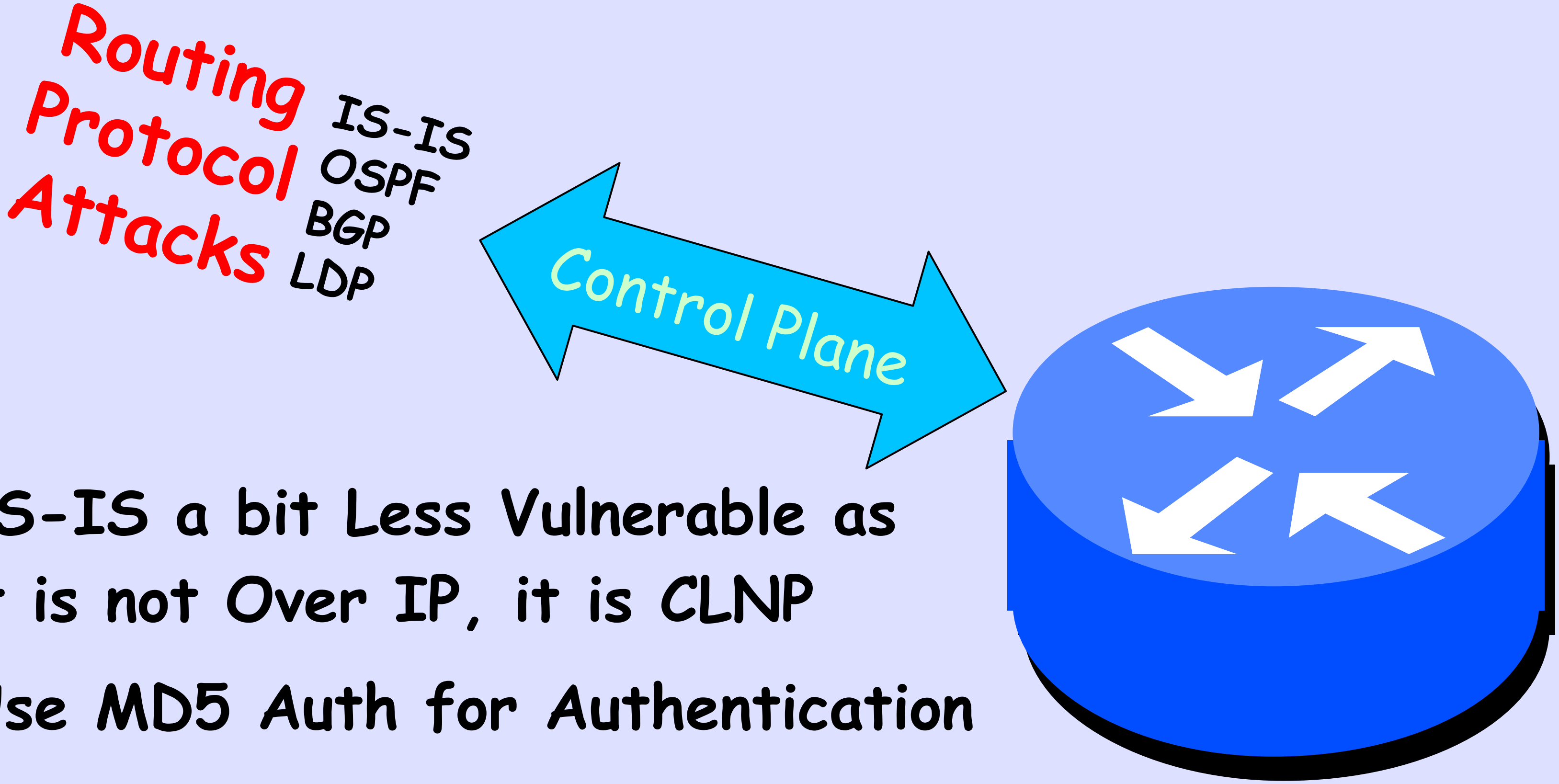
ACLs

Access Control Lists

NTP ACLs

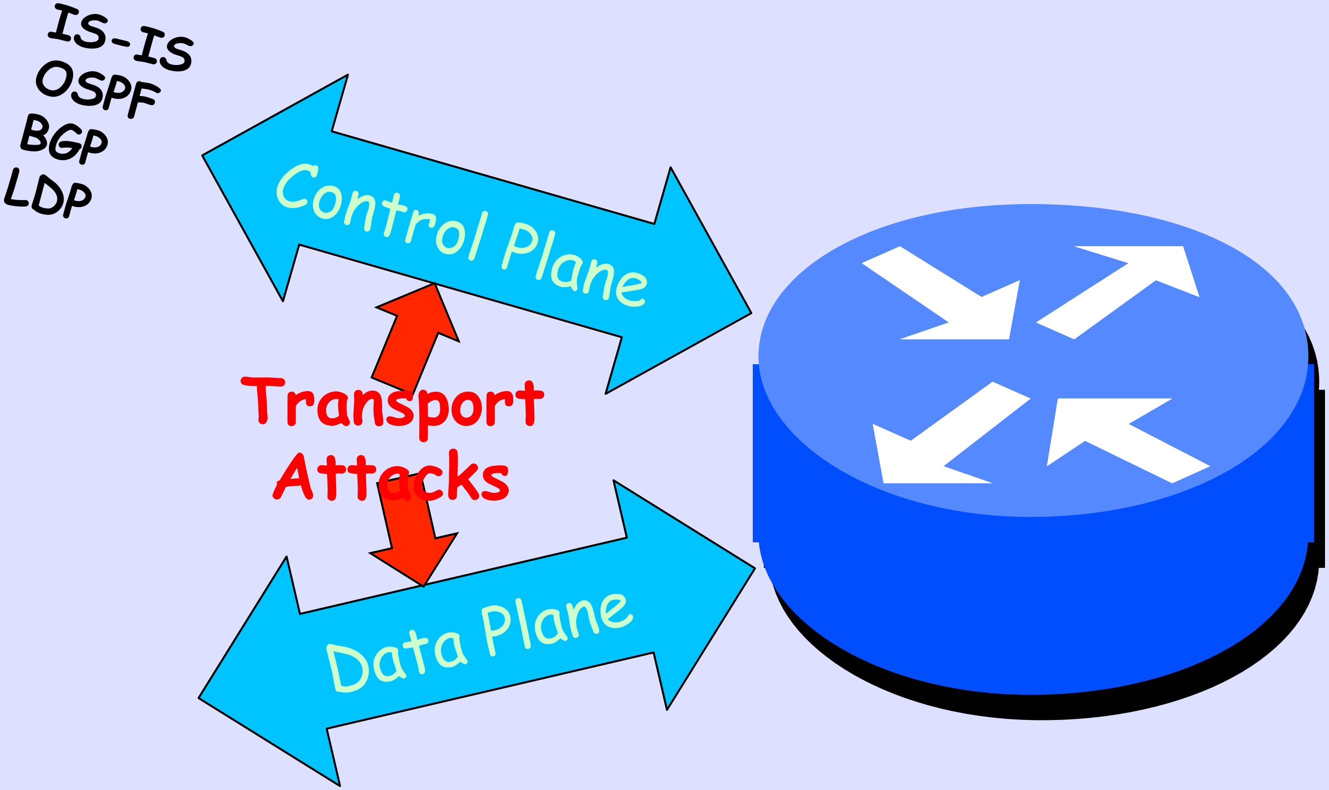
```
! Core NTP configuration
ntp server 209.20.186.192                          ! ntp.psg.com
ntp server 147.28.0.36                             ! rip.psg.com
ntp server 147.28.0.62                             ! psg.com
!
ntp source Loopback0
!
access-list 46 remark utility ACL to block everything
access-list 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
```

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



- 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 Auth

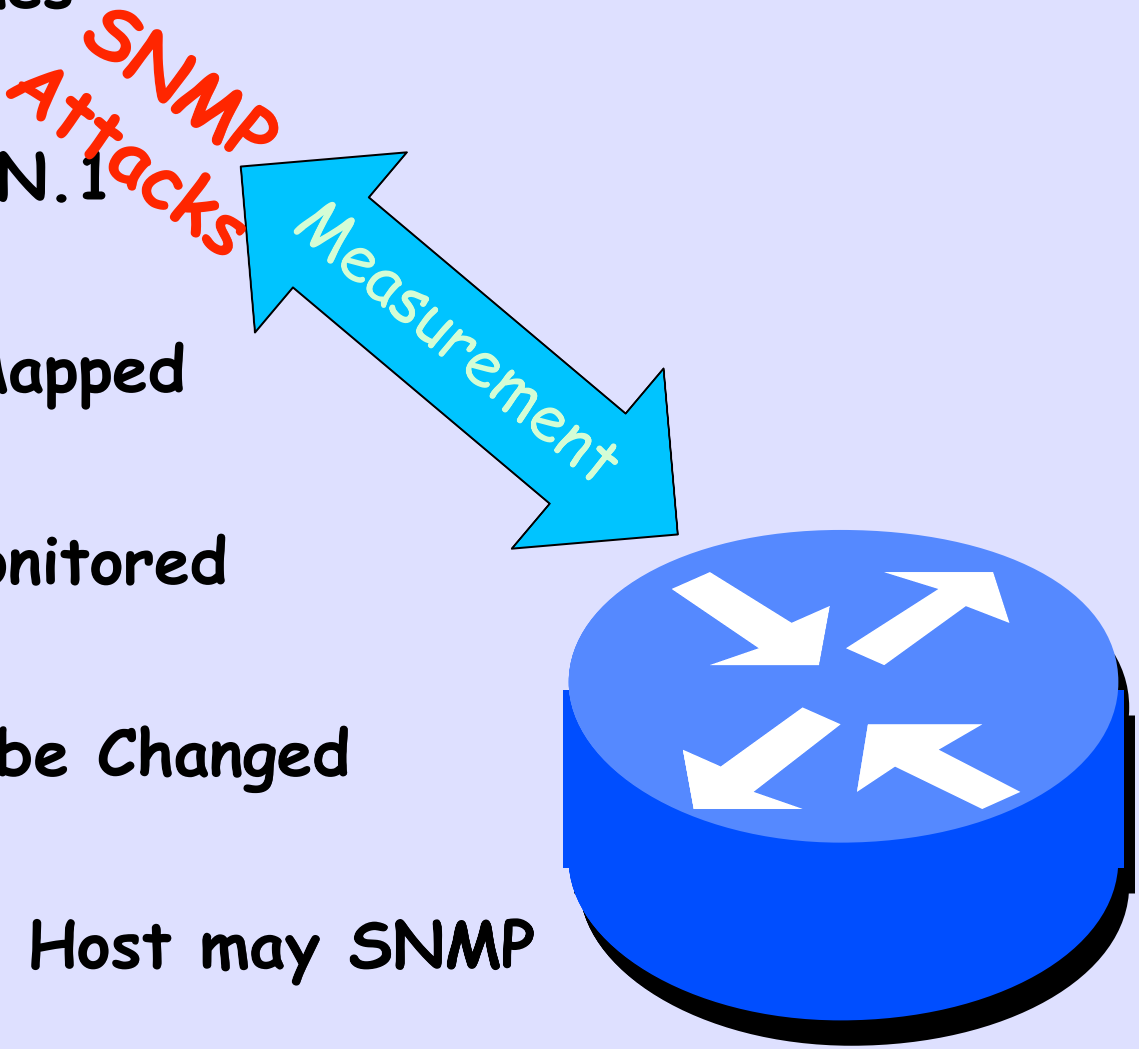
```
neighbor 199.238.113.9 remote-as 2914

neighbor 199.238.113.9 description verio 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

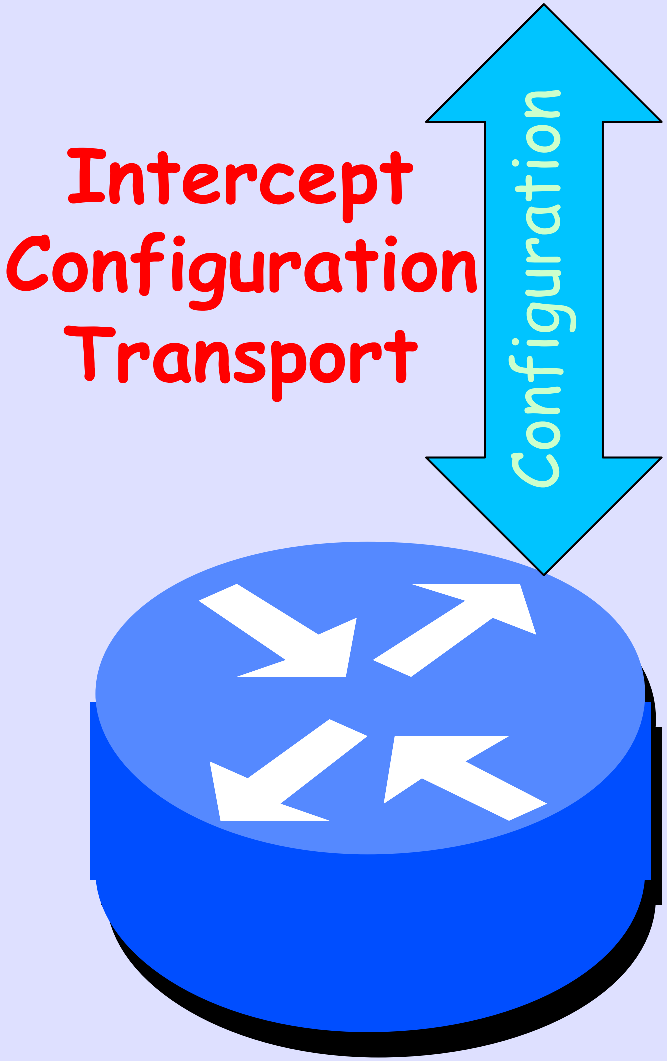
- Occasional New Ones
- Usually against ASN.1
- Network may be Mapped
- Traffic may be Monitored
- Configuration may be Changed
- Use ACLs on What Host may SNMP
- Defense is Using SNMPv3 which is Encrypted



Simple SNMP Precaution

```
! snmp pollers
access-list 98 permit 129.250.32.0 0.0.0.255
access-list 98 permit 129.250.42.0 0.0.0.63
access-list 98 permit 147.28.0.35
access-list 98 permit 147.28.0.60
!
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server enable traps envmon
snmp-server community <secret> RO 98
```

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



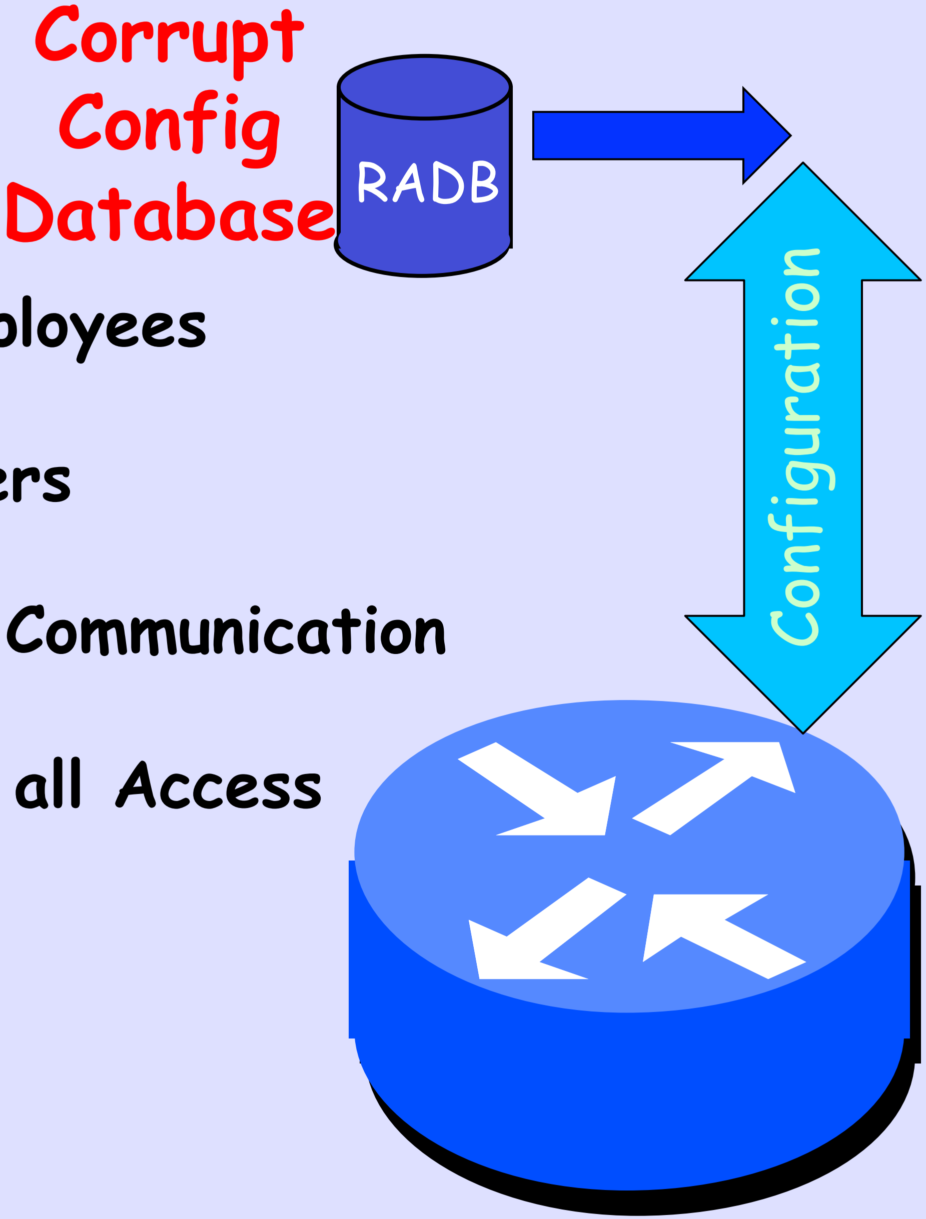
ssh Access Control List

```
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
```

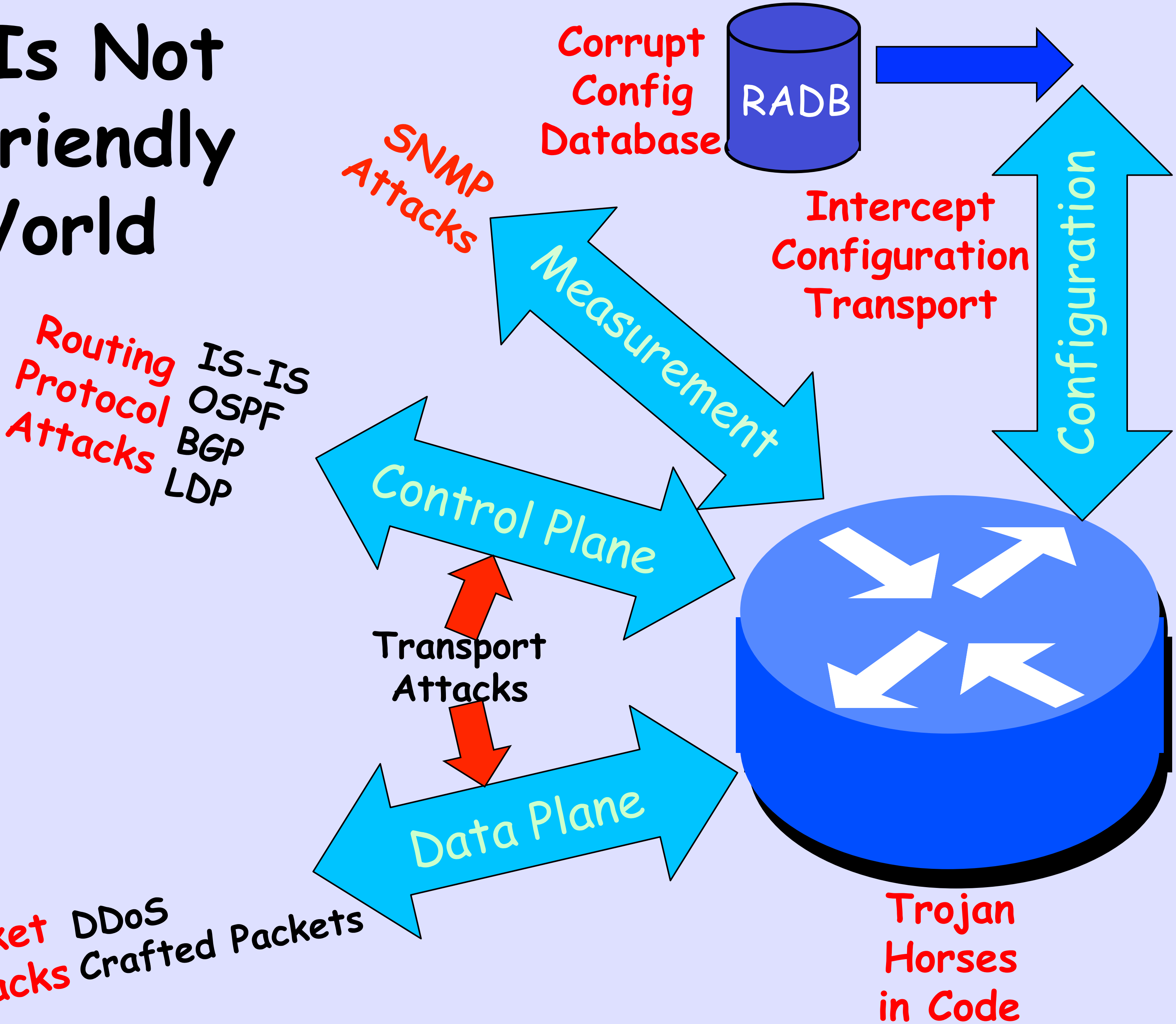
```
ip access-list standard vty4
 permit 147.28.0.0      0.0.7.255
 permit 198.180.150.0   0.0.0.255
 permit 198.180.152.0   0.0.0.255
!
ipv6 access-list vty6
 permit ipv6 2001:418:1::/48 any
```

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

- Protect Your Provisioning
- Against Intrusion and Employees
- Isolate and Protect Servers
- Secure All Inter-System Communication
- Two-Factor Authenticate all Access



It Is Not A Friendly World



Corrupt Config Database

SNMP Attacks

Intercept Configuration Transport

Routing Protocol Attacks IS-IS OSPF BGP LDP

Transport Attacks

Packet Attacks DDoS Crafted Packets

Trojan Horses in Code