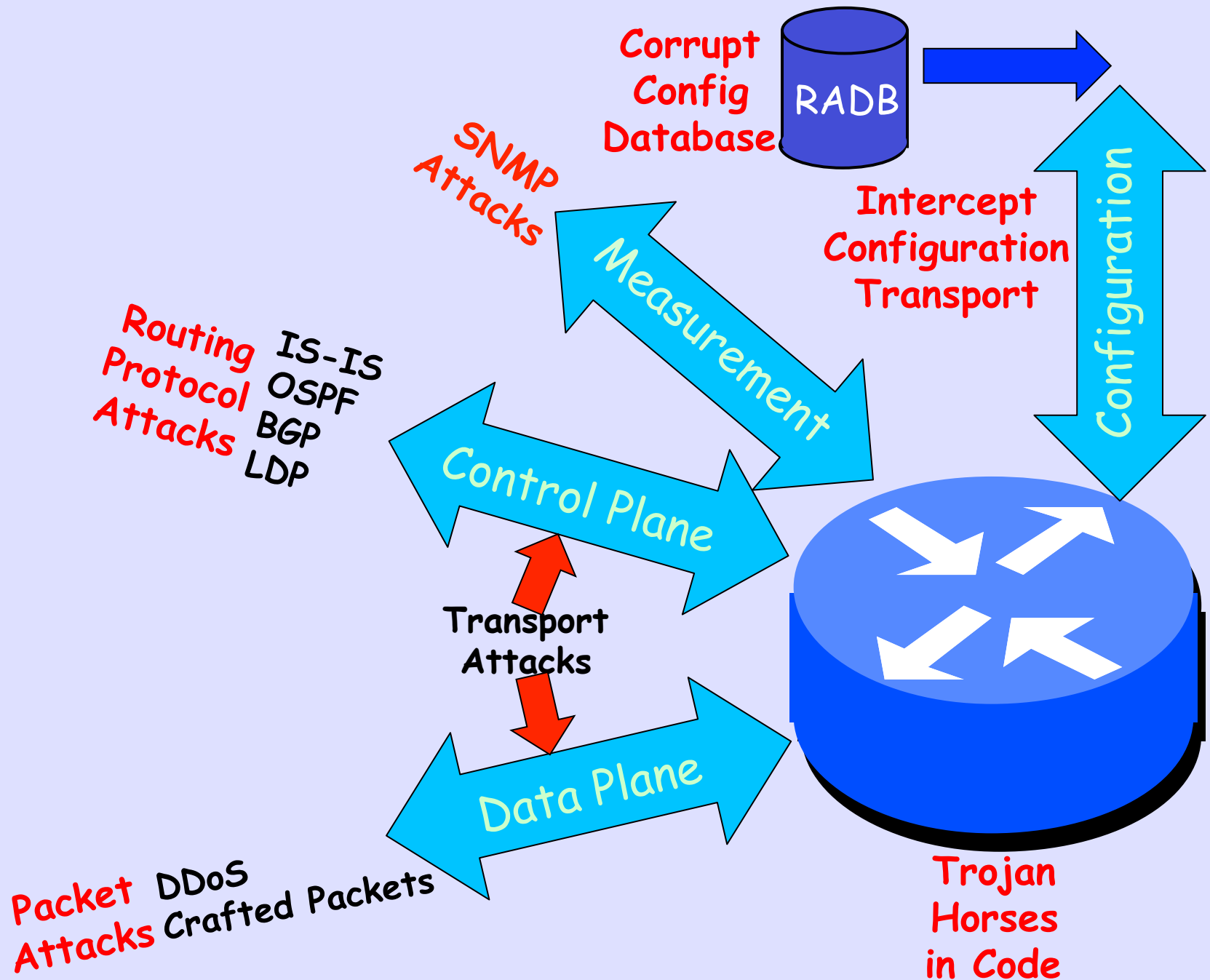


2-3-1

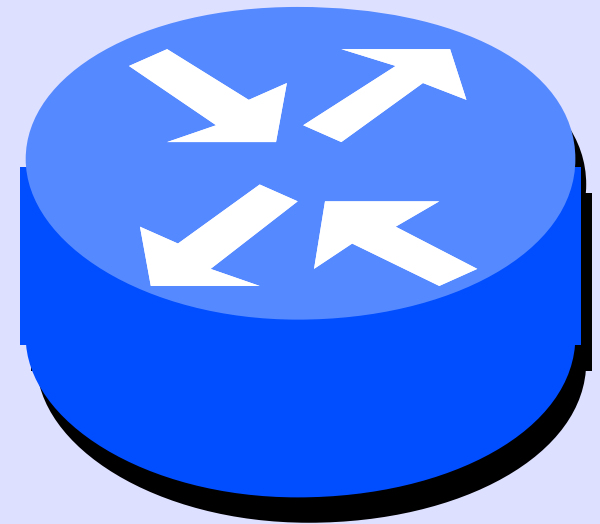
Protecting

Network Infrastructure

Routers, Switches, etc.

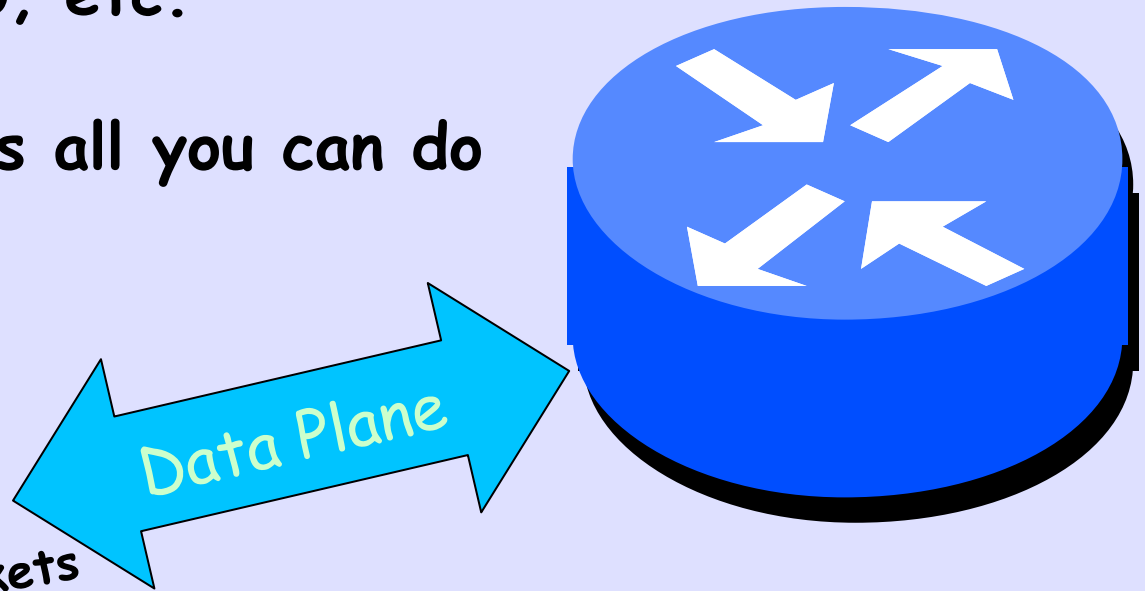


- Could Spy on Protocols, Data, or Configuration
- Could Alter Protocols, Data, or Configuration
- Would Require Vendor Collusion
- Nation State Attack
- Considered Unlikely
- Only Protection is Code Audit



**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

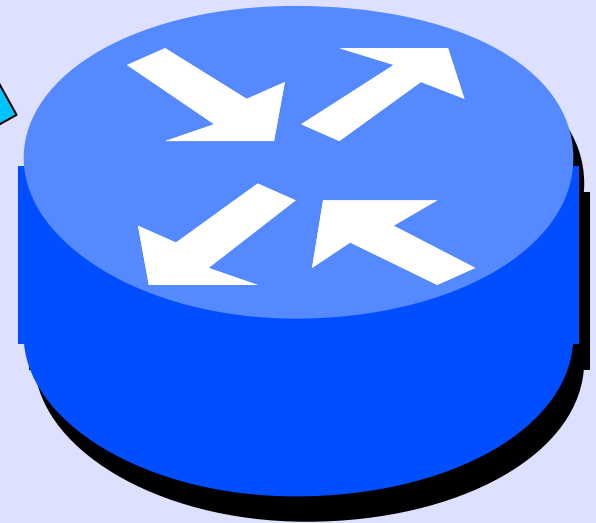
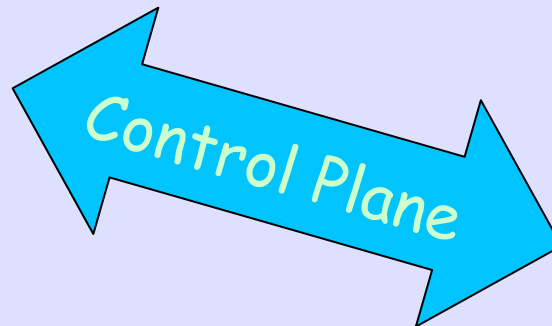


Packet Attacks DDoS
Crafted Packets

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

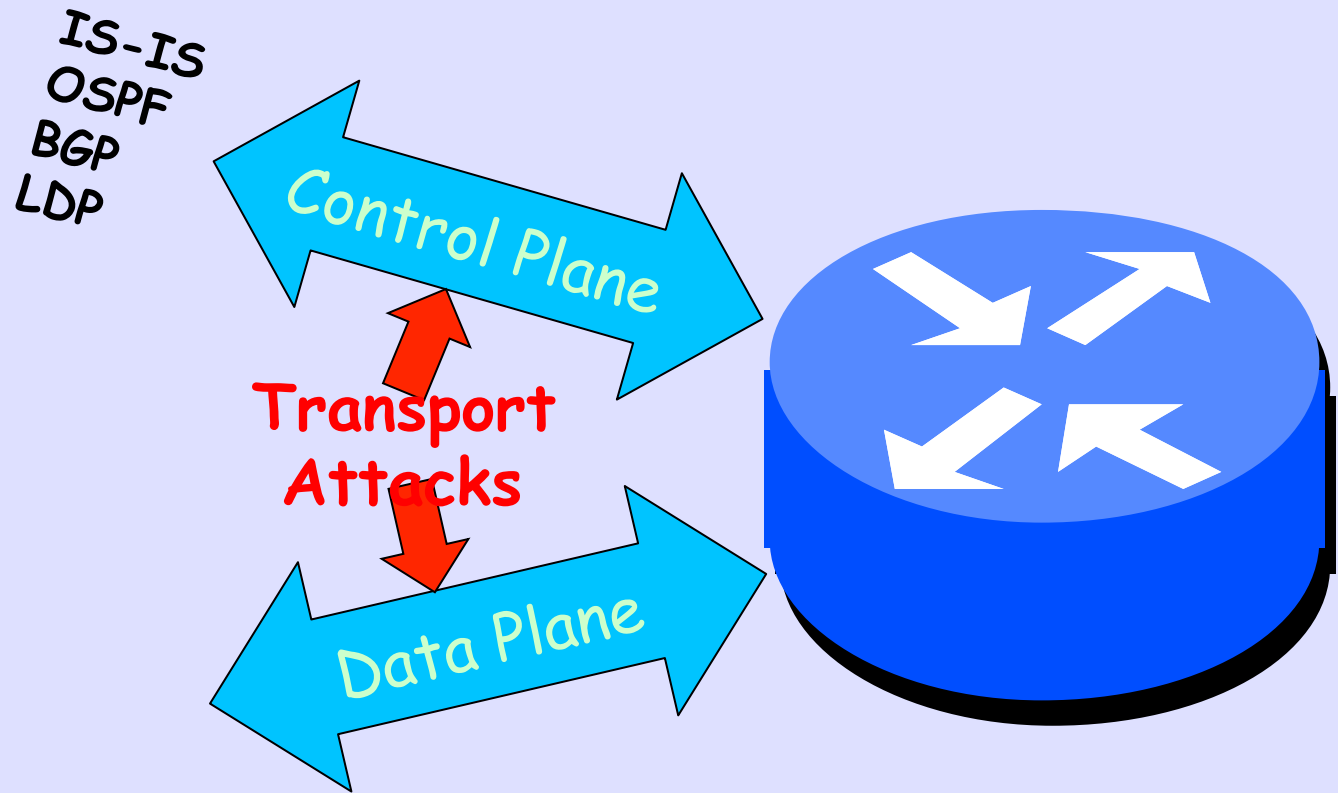
**Routing
Protocol
Attacks**

IS-IS
OSPF
BGP
LDP



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

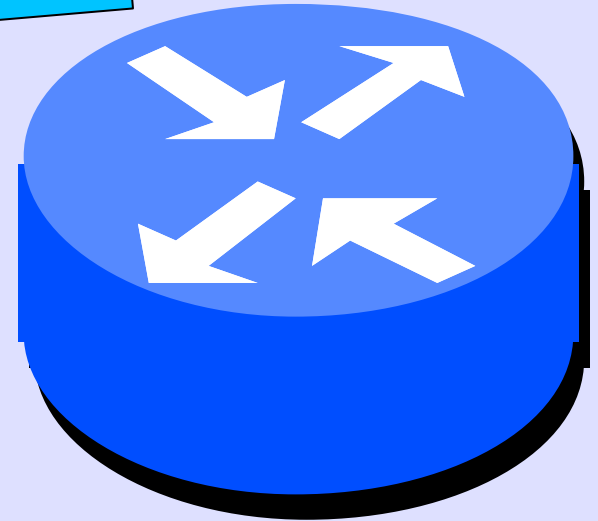
- Assume Monkeys are in the Middle
- Authenticate all Control Traffic, MD5 or Stronger
- Teach Customers to Encrypt: https, imaps, ssh, ...
- WPA2 on WiFi



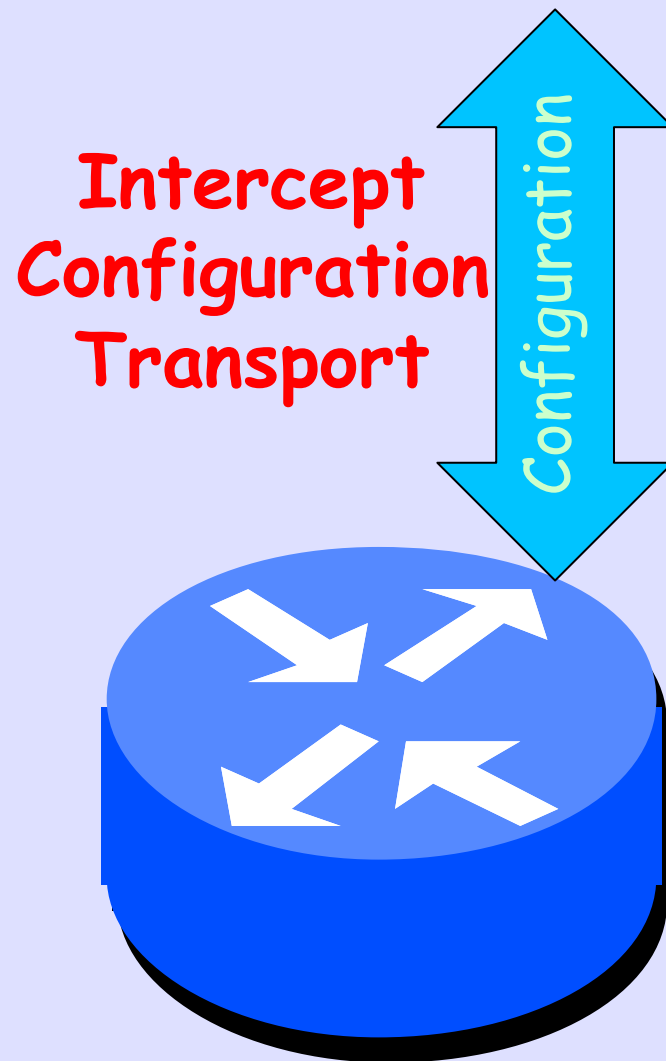
- Occasional New Ones
- Usually against ASN.1
- Network may be Mapped
- Traffic may be Monitored
- Configuration may be Changed
- Use ACLs on What Host may SNMP
- Defense is Using SNMPv3 which is Encrypted

SNMP
Attacks

Measurement

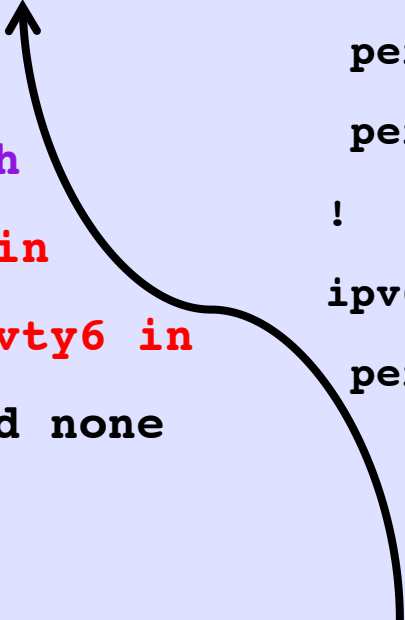


- Tapping Configuration Session
 - Stealing Password
 - Stealing Configuration
- DO NOT USE Telnet
- Configure Over ssh
- Restrict ssh to Special Hosts



ssh Access Control List

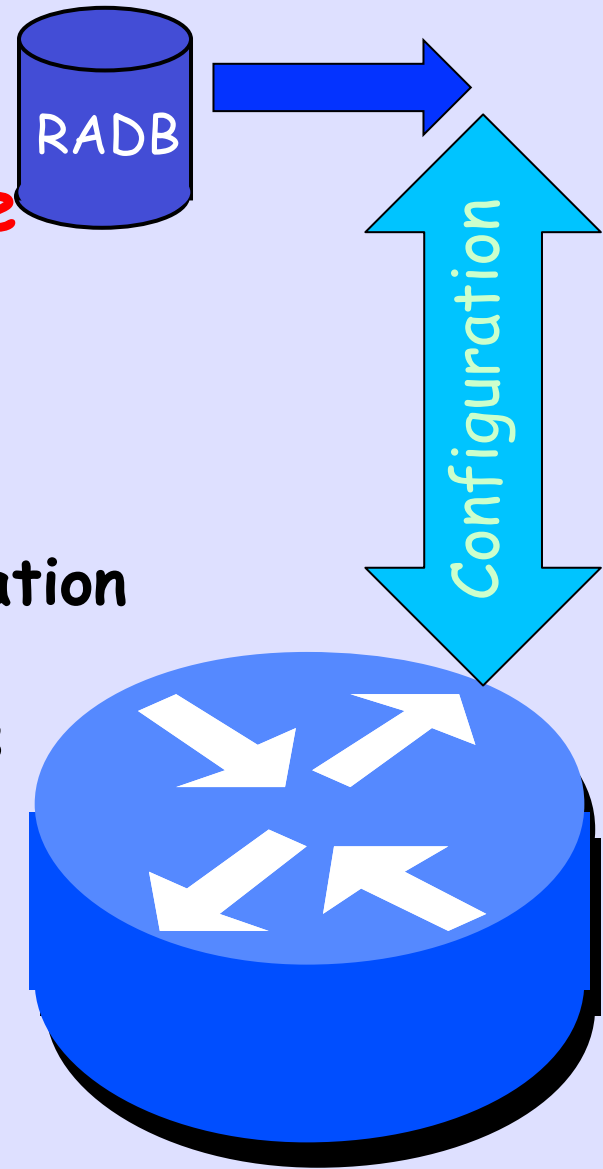
```
line vty 0 4                                ip access-list standard vty4
password 7 071C205F4600140C5C          permit 147.28.0.0      0.0.7.255
exec-timeout 0 0                          permit 198.180.150.0   0.0.0.255
transport input ssh                       permit 198.180.152.0   0.0.0.255
access-class vty4 in                      !
ipv6 access-list vty6                     permit ipv6 2001:418:1::/48 any
ipv6 access-class vty6 in
transport preferred none
```



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

**Corrupt
Config
Database**



It Is Not A Friendly World

