

# Hardening IPv6 Network Devices

## ISP Workshops



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license (<http://creativecommons.org/licenses/by-nc/4.0/>)

# Acknowledgements

---

- This material originated from the Cisco ISP/IXP Workshop Programme developed by Philip Smith & Barry Greene
  - These slides were developed by Dean Pemberton
  
- Use of these materials is encouraged as long as the source is fully acknowledged and this notice remains in place
  
- Bug fixes and improvements are welcomed
  - Please email *workshop (at) bgp4all.com*

Philip Smith

# Agenda

---

- ❑ Limiting Device Access
- ❑ Secure SNMP Access
- ❑ Securing the Data Path
- ❑ Configuration and Archiving

# Limiting Device Access



# Think of ALL Devices

---

- The following problem was reported in 2013 and affects low-end CPEs (ADSL connections only)
  - Admin password exposed via web interface
  - Allow WAN management (this means anyone on Internet)
  - Bug fixed and reintroduced depending on the firmware version
- The bug is quite a number of years old

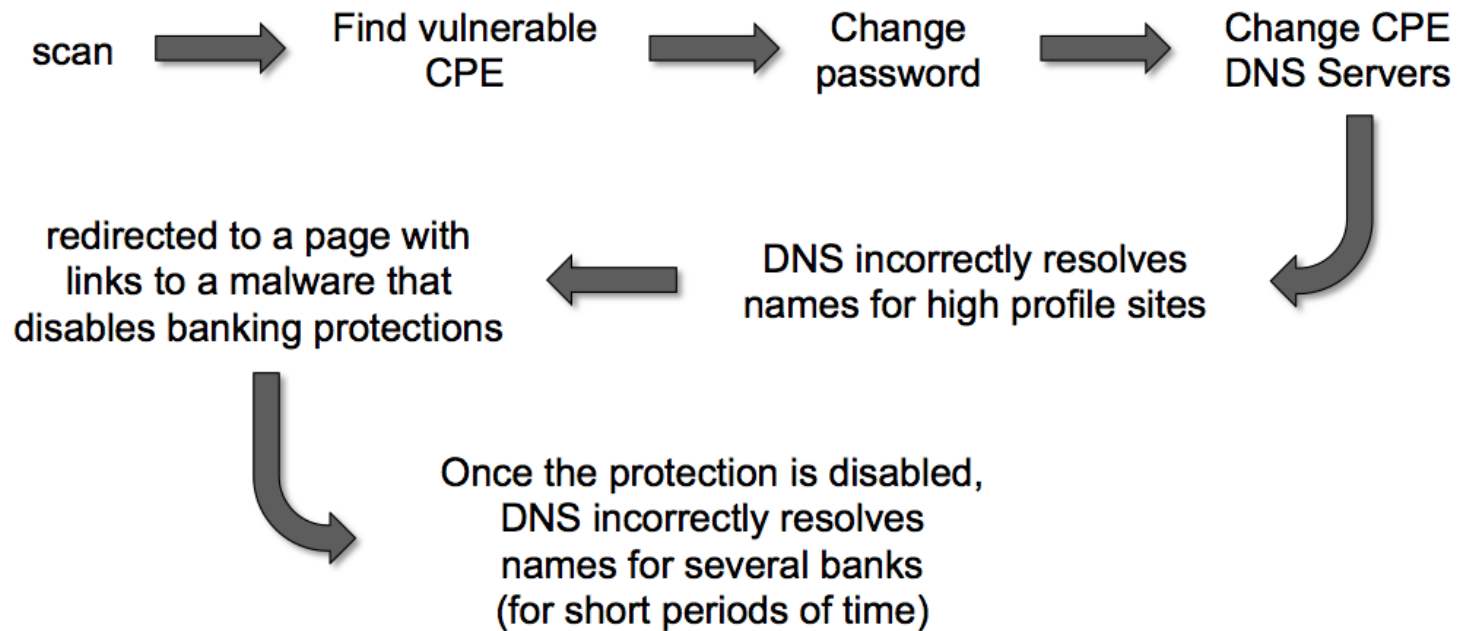
# Password Visible via Web Interface

The image shows a web browser window with the address bar displaying '189. password.cgi'. The page content is titled 'Access Control -- Passwords' and contains a form with fields for 'Username:', 'Old Password:', 'New Password:', and 'Confirm Password:'. The text on the page explains that access to the DSL router is controlled and lists user permissions for 'admin', 'support', and 'user'. An inset window shows the source code of the page, which includes a hidden section containing the following JavaScript code:

```
1 <html>
2   <head>
3     <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
4     <link rel="stylesheet" href='stylemain.css' type='text/css'>
5     <link rel="stylesheet" href='colors.css' type='text/css'>
6     <script language="javascript" src="util.js"></script>
7     <script language="javascript">
8   <!-- hide
9
10  pwdAdmin = 'admin';
11  pwdSupport = 'support';
12  pwdUser = 'user';
13
14  function btnApply() {
15    var loc = 'password.cgi?';
16
17    with ( document.forms[0] ) {
18      var idx = userName.selectedIndex;
19      switch ( idx ) {
20        case 0:
21          alert("No username is selected.");
22          return;
```

# How CPE are Exploited

---



# Magnitude of Problem

---

- 4.5 Million CPEs (ADSL Modems) using a unique malicious DNS
- In early 2012 more than 300,000 CPEs still infected
- 40 malicious DNS servers found
  
- Could device hardening have made a difference?



# Device Physical Access

---

- Equipment kept in highly restrictive environments
- Console access
  - password protected
  - access via OOB management
  - configure timeouts
- Individual users authenticated
- Social engineering training and awareness
  
- “If you can touch it... the device now belongs to you”

# Interface Hardening

---

## □ IPv4

- no ip proxy-arp
- no ip unreachable
- no ip redirects
- no ip directed-broadcast
- no ip mask-reply

## □ IPv6

- no ipv6 unreachable
- no ipv6 redirects

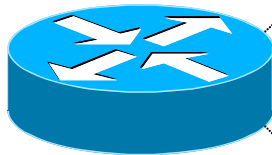
# Device Access Control

---

- ❑ Set passwords to something not easily guessed
- ❑ Use single-user passwords (avoid group passwords)
- ❑ Encrypt the passwords in the configuration files
- ❑ Use different passwords for different privilege levels
- ❑ Use different passwords for different modes of access
- ❑ IF AVAILABLE – use digital certificate based authentication mechanisms instead of passwords

# Secure Access with Passwords and Logout Timers

---



```
line console 0
login
password console-pw
exec-timeout 1 30
line vty 0 4
login
password vty-pw
exec-timeout 5 0
!
enable secret enable-secret
username dean secret dean-secret
```

# Never Leave Passwords in Clear-Text

---

- ❑ service password-encryption command
- ❑ password command
  - Will encrypt all passwords on the Cisco IOS
  - with Cisco-defined encryption type "7"
  - Use "command password 7 <password>" for cut/paste operations
  - Cisco proprietary encryption method
- ❑ secret command
  - Uses MD5 to produce a one-way hash
  - Cannot be decrypted
  - Use "command secret 5 <password>"
  - to cut/paste another "enable secret" password

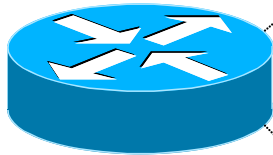
# Management Plane Filters

---

- Authenticate Access
- Define Explicit Access To/From Management Stations
  - SNMP
  - Syslog
  - TFTP
  - NTP
  - AAA Protocols
  - DNS
  - SSH, Telnet, etc.

# Authenticate Individual Users

---



```
username dean secret dean-secret  
username miwa secret miwa-secret  
username pfs secret pfs-secret  
username staff secret group-secret
```

***Do NOT have group passwords!***

# User Authentication: Good

---

- From Cisco IOS 12.3, MD5 encryption was added for user passwords
  - **Do NOT use type 7 encryption**
    - (it is easy to reverse)

```
aaa new-model
aaa authentication login neteng local
username pfs secret 5 $1$j6Ac$3KarJszBV3VMaL/2Nio3E.
username dean secret 5 $1$LPV2$Q04NwAudy0/4AHHQHvWj0
line vty 0 4
  login neteng
  access-class 3 in
```



# User Authentication: Better

---

- Use centralised authentication system
  - RADIUS (not recommended for system security)
  - TACACS+

```
aaa new-model
aaa authentication login default group tacacs+ enable
aaa authentication enable default group tacacs+ enable
aaa accounting exec start-stop group tacacs+
!
ip tacacs source-interface Loopback0
tacacs server IPv6-TP
  address ipv6 2001:DB8::1
  key CKr3t#
tacacs server IPv4-TP
  address ipv4 192.168.1.1
  key CKr3t#
line vty 0 4
  access-class 3 in
```

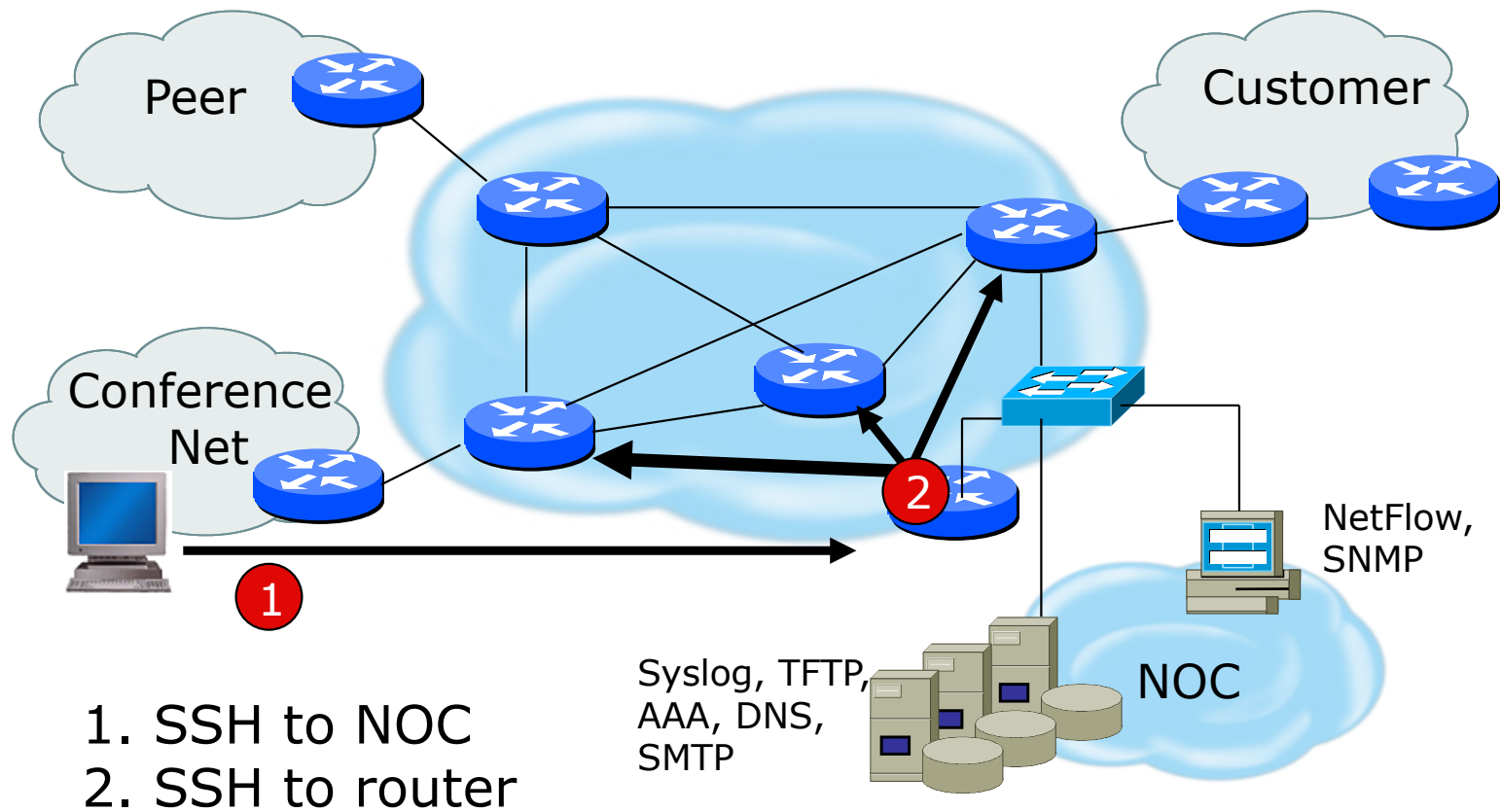
# Restrict Access To Trusted Hosts

---

- Use filters to specifically permit hosts to access an infrastructure device
- Example:

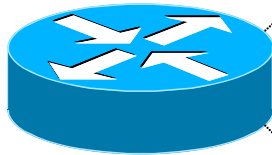
```
ip access-list extended VTY
 permit tcp host 192.168.200.7 192.168.1.0 0.0.0.255 eq 22 log-input
 permit tcp host 192.168.200.8 192.168.1.0 0.0.0.255 eq 22 log-input
 permit tcp host 192.168.100.6 192.168.1.0 0.0.0.255 eq 23 log-input
 deny ip any any log-input
!
line vty 0 4
 access-class VTY in
 transport input ssh telnet
```

# Using an SSH 'Jumphost'



# Banner – What Is Wrong ?

---



```
banner login ^C
```

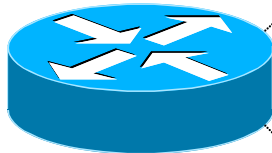
```
    You should not be on this device.
```

```
    Please Get Off My Router!!
```

```
^C
```

# More Appropriate Banner

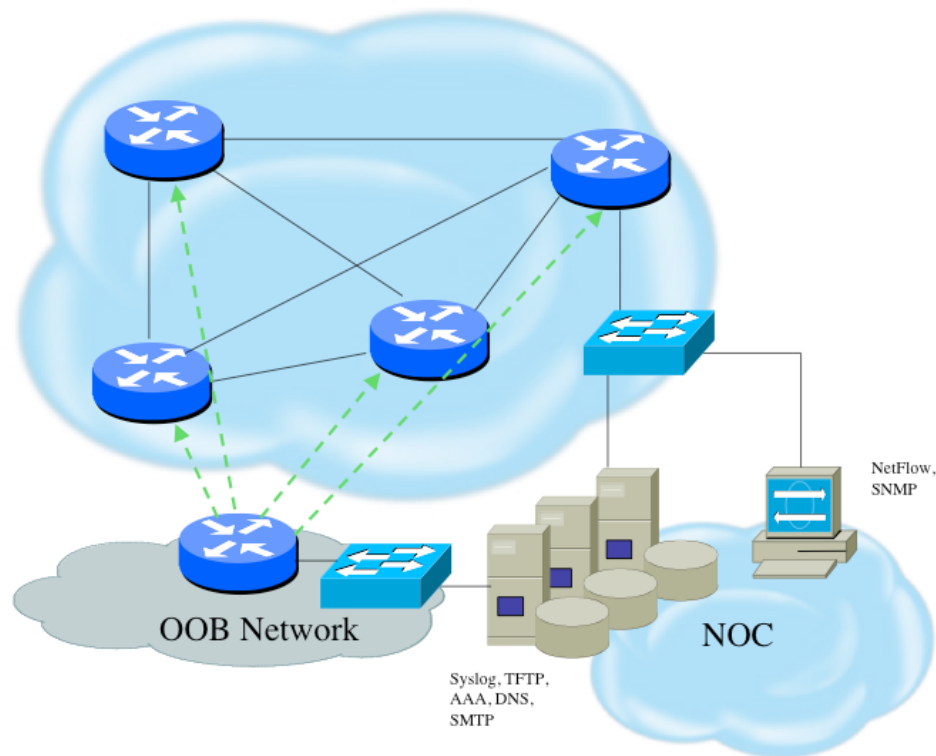
---



**!!!! WARNING !!!!**  
You have accessed a restricted device.  
All access is being logged and any  
unauthorized access will be prosecuted  
to the full extent of the law.

# Device OOB Management

---



- ❑ Out-of-band device management should be used to ensure DoS attacks do not hinder getting access to critical infrastructure devices
- ❑ Dial-back encrypted modems are sometimes still used as backup

# Device Management Common Practice (1)

---

- SSH used exclusively
  - Do NOT use Telnet, not even from Jump hosts
- HTTP and HTTPS access explicitly disabled
- All access authenticated
  - Varying password mechanisms
  - AAA usually used
    - Different servers for in-band vs OOB
    - Different servers for device authentication vs other
    - Static username pw or one-time pw
  - Single local database entry for backup

## Device Management Common Practice (2)

---

- Each individual has specific authorization
- Strict access control via filtering
- Access is audited with triggered pager/email notifications
- SNMP is read-only
  - Restricted to specific hosts
  - View restricted if capability exists
  - Community strings updated every 30-90 days



# Turn Off Unused Services

---

## □ Global Services

- no service finger (before Cisco IOS 12.0)
- no ip finger
- no service pad
- no service udp-small-servers
- no service tcp-small-servers
- no ip bootp server
- no cdp run

## □ Interface Services

- no ip redirects
- no ip directed-broadcast
- no ip proxy arp
- no cdp enable

# Secure SNMP Access



# Secure SNMP Access

---

- ❑ SNMP is primary source of intelligence on a target network!
- ❑ Block SNMP from the outside

```
access-list 101 deny udp any any eq snmp
```

- ❑ If the router has SNMP, protect it!

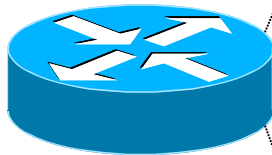
```
snmp-server community f00bAr RO 8  
access-list 8 permit 127.1.3.5
```

- ❑ Explicitly direct SNMP traffic to an authorized management station.

```
snmp-server host f00bAr 127.1.3.5
```

# Secure SNMP Access

---



```
ipv6 access-list SNMP-PERMIT
 permit ipv6 2001:DB8:22::/64 any
 permit ipv6 any 2001:DB8:22::/64
!
no snmp community public
no snmp community private
!
snmp-server enable traps
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server trap-source Loopback0
snmp-server community v6comm RO ipv6 SNMP-PERMIT
```

# SNMP Best Practices

---

- ❑ Do not enable read/write access unless really necessary
  - Read – for access by Networking Monitoring System (eg LibreNMS)
  - Write – never!
- ❑ Choose community strings that are difficult to guess
  - Use same algorithm as for passwords
- ❑ Limit SNMP access to specific IP addresses
- ❑ Limit SNMP output with views

# Secure Logging Infrastructure

---

- ❑ Log enough information to be useful but not overwhelming.
- ❑ Create backup plan for keeping track of logging information should the syslog server be unavailable
- ❑ Remove private information from logs
- ❑ How accurate are your timestamps?
  - NTP needs to be configured
  - Synchronise with trusted time sources, eg [pool.ntp.org](http://pool.ntp.org) or GPS receivers

# Fundamental Device Protection Summary

---

- ❑ Secure logical access to routers with passwords and timeouts
- ❑ Never leave passwords in clear-text
- ❑ Authenticate individual users
- ❑ Restrict logical access to specified trusted hosts
- ❑ Allow remote vty access only through ssh
- ❑ Disable device access methods that are not used
- ❑ Protect SNMP if used
- ❑ Shut down unused interfaces
- ❑ Shut down unneeded services
- ❑ Ensure accurate timestamps for all logging
- ❑ Create appropriate banners
- ❑ Test device integrity on a regular basis

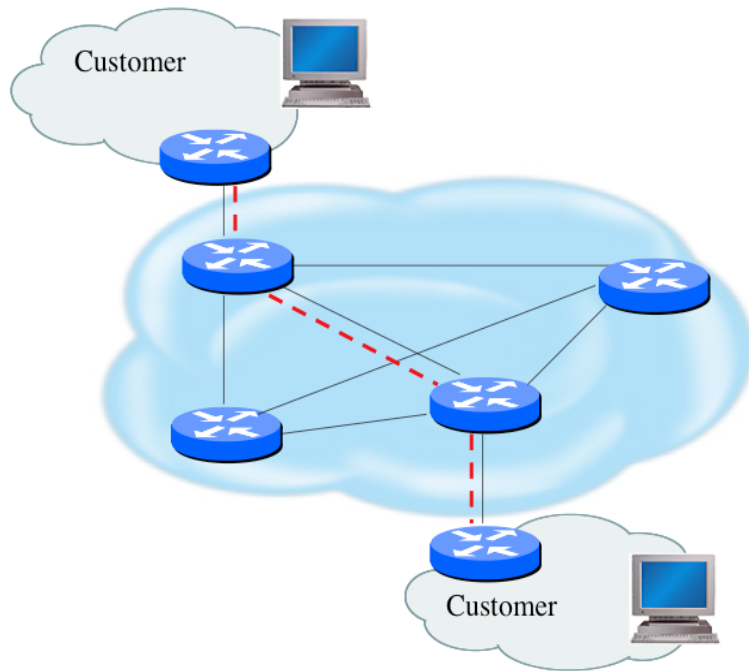
# Securing the Data Path





# Securing The Data Path

---



- ❑ Filtering and rate limiting are primary mitigation techniques
- ❑ Edge filter guidelines for ingress filtering (BCP38/BCP84)
- ❑ Null-route and black-hole any detected malicious traffic
- ❑ Netflow is primary method used for tracking traffic flows
- ❑ Logging of Exceptions

# Data Plane (Packet) Filters

---

- Most common problems
  - Poorly-constructed filters
  - Ordering matters in some devices
- Scaling and maintainability issues with filters are commonplace
- Make your filters as modular and simple as possible
- Take into consideration alternate routes
  - Backdoor paths due to network failures

# Filtering Deployment Considerations

---

- ❑ How does the filter load into the router?
- ❑ Does it interrupt packet flow?
- ❑ How many filters can be supported in hardware?
- ❑ How many filters can be supported in software?
- ❑ How does filter depth impact performance?
- ❑ How do multiple concurrent features affect performance?
- ❑ Do I need a standalone firewall?

# General Filtering Best Practices

---

- ❑ Explicitly deny all traffic and only allow what you need
- ❑ The default policy should be that if the firewall doesn't know what to do with the packet, deny/drop it
- ❑ Don't rely only on your firewall for all protection of your network
- ❑ Implement multiple layers of network protection
- ❑ Make sure all of the network traffic passes through the firewall
- ❑ Log all firewall exceptions (if possible)

# Ingress Filtering



```
ipv6 access-list INBOUND-iACL
remark Permit the legitimate signaling traffic (BGP, EIGRP, PIM)
permit tcp host 2001:db8:20::1 host 2001:db8:20::2 eq bgp
permit tcp host 2001:db8:20::1 eq bgp host 2001:db8:20::2
permit 88 any any
permit 103 any any
remark Permit NDP packets
permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation
remark Deny RHO and other unknown extension headers
deny ipv6 any any routing-type 0 log
deny ipv6 any any log undetermined-transport
remark Permit the legitimate management traffic
permit tcp 2001:db8:11::/48 any eq 22
permit tcp 2001:db8:11::/48 any eq www
permit udp 2001:db8:11::/48 any eq snmp
remark Deny any packets to the infrastructure address space
deny ipv6 any 2001:db8:2222::/48
deny ipv6 any 2001:db8:20::/48
permit ipv6 any any
!
interface FastEthernet 0/0
description Connection to outside network
ipv6 address 2001:db8:20::2/64
ipv6 traffic-filter INBOUND-iACL in
```

# RFC2827 (BCP38) – Ingress Filtering

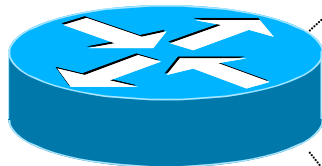
---

- ❑ If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.
- ❑ The ONLY valid source IP address for packets originating from a customer network is the one assigned by the ISP (whether statically or dynamically assigned).
- ❑ An edge router could check every packet on ingress to ensure the user is not spoofing the source address on the packets which he is originating.

# But What About Egress Filtering?

---

- ❑ In theory, certain addresses should not be seen on the global Internet
- ❑ In practice they are, and filters aren't being deployed (even when capability available)



```
ipv6 access-list DSL-ipv6-Outbound
permit ipv6 2001:DB8:AA65::/48 any
deny  ipv6 any any log

interface atm 0/0
  ipv6 traffic-filter DSL-ipv6-Outbound out
```

# Configuration and archiving





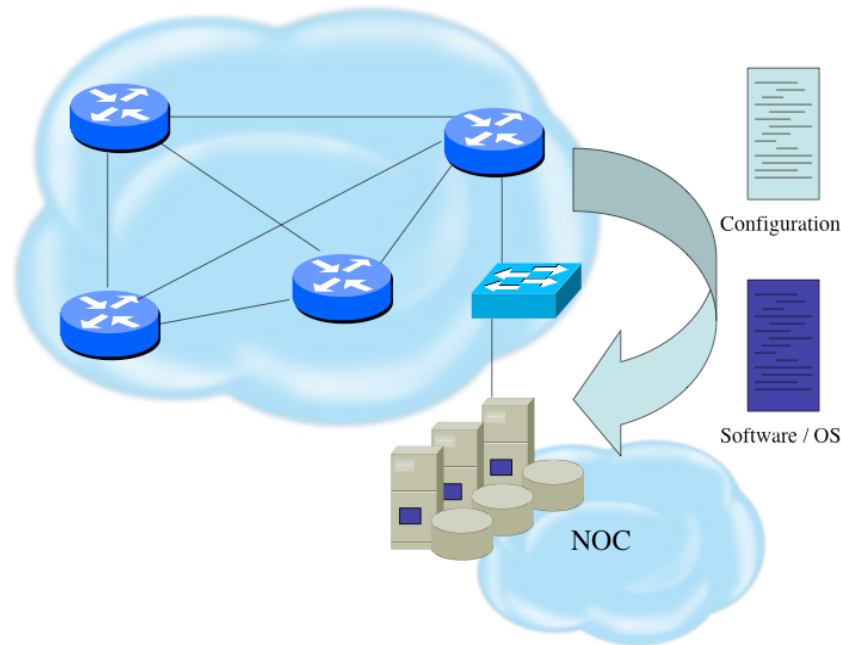
# System Images and Configuration Files

---

- ❑ Careful of sending configurations where people can snoop the wire
  - CRC or MD5 validation
  - Sanitize configuration files
- ❑ SCP should be used to copy files
  - TFTP and FTP should be avoided
- ❑ Use tools like 'RANCID' to periodically check against modified configuration files

# Software and Configuration Upgrade / Integrity

---



- ❑ Files stored on specific systems with limited access
- ❑ All access to these systems are authenticated and audited
- ❑ SCP is used where possible; FTP is NEVER used; TFTP still used
- ❑ Configuration files are polled and compared on an hourly basis (RANCID)
- ❑ Filters limit uploading / downloading of files to specific systems
- ❑ Many system binaries use MD-5 checks for integrity
- ❑ Configuration files are stored with obfuscated passwords

# Infrastructure Security Summary

---

- ❑ Every device in your network could be exploited so make sure to harden them all (especially change default username/passwords)
  - Printers, tablets, CPE's, etc
- ❑ Understand what you are sending in the clear from sending device to recipient and protect where needed
- ❑ Log and audit for trends since sometimes an abnormality can show the start of reconnaissance for a later attack

# Hardening IPv6 Network Devices



ISP Workshops