IOS Configurations…
What Should Be in Them, but Sometimes Isn’t!

Who Should Attend?

- Engineers from enterprise networks
- Consultants in charge of the security and administration policy of a routers network
- Anyone else interested in starting the operations of a routers network
Our Playground

Enterprise  CPE  Provider

DMZ  Internet

Agenda

- Basic Commands
- Network Management
- Administration
- Security
- Summary
Basic Commands

Hostname

- Give your routers a meaningful name
- Format should be defined in your policy
- If you have a DNS, put it in the DNS

hostname NYCore7200
Interface Description

- Give meaningful descriptions on your interfaces
- Allows for self documentation of the router configs
  ```
  interface Serial0
  description Frame Relay link to Carrier line ABCD
  ```
  ```
  interface serial 0.1 point-to-point
  description link to NYCore7200
  ```

Bandwidth

- Some routing protocols use bandwidth to make routing decisions
- Useful documenting tool
  ```
  interface serial0
  bandwidth 64
  ```
Use Loopback Interfaces

- A loopback interface is generally up as long as the device is operational
- Simplify the management: logging, SNMP, etc.
- Solid entity for router ID, BGP update-source, etc.

```plaintext
interface Loopback0
description OSPF, BGP, SNMP
ip address 1.2.3.4 255.255.255.255
```

DNS

- If no DNS, turn off domain lookup
  ```plaintext
  no ip domain-lookup
  ```
- If there is a DNS set it up
  ```plaintext
  ip domain-list cisco.com, east.cisco.com
  ip name-server 1.2.3.4 5.6.7.8
  ```
- Add router interfaces to the DNS
  It makes things easier when tracing routes
Turn on CDP

- Quick reference to router and switch adjacencies
- Normally on by default
- Don’t enable CDP on external interfaces
  
  ```
  interface Serial0
  no cdp enable
  ```
- Some of Cisco’s network management tools use CDP for discovery
  
  CW2000 uses CDP to create the topology map

Interface Stats

- Need a more granular output for show interface
  
  ```
  Show interface calculates on a 5 minute average
  Useful for seeing peaks in traffic
  ```
  
  ```
  interface serial0
  load-interval 30
  ```

Remember: Turn It off When Finished!
Network Time Protocol

- Get your routers time in sync (logging/debug)
- Use NTP
  - From external time source
  - From internal time source
  - Router can act as stratum 1 time source

NTP Configuration

- Set time zone
  - clock timezone <name> [+/hours [mins]]
- Router a source
  - ntp master 1
- External time source (master)
  - ntp server a.b.c.d
- External time source (equivalent)
  - ntp peer e.f.g.h
NTP Example

- Configuration example
  
  clock timezone PST –8  
  ntp server 1.2.3.4  
  ntp peer 5.6.7.8  
  ntp authenticate

Loading Configurations

- Where do you load them from?  
  NVRAM, Flash, TFTP, FTP
  
  boot network tftp://1.2.3.4/tftpboot/network-confg
  boot host tftp://1.2.3.4/tftpboot/hostname-confg

- If your policy doesn’t allow the routers to retrieve their configuration via TFTP, turn off the service
  no service config
Loading Images

- Where do you load them from?
  - Flash, TFTP, FTP, ROM
    - `boot system flash`
    - `boot system tftp://1.2.3.4/c2600-i-mz.121-5.T4`
    - `boot system rom`

Config-Register

- 2 byte configuration register stored in NVRAM
- Are you loading an operating system image?
  - `config-register 0x0000`
  - `config-register 0x2101`
  - `config-register 0x2102`
- Platform specific part
**Flash Memory**

- Buy enough Flash to hold 2 Cisco IOS® images
- Allow for some growth of IOS image
- For devices without a FLASH file system, have enough FLASH to enable it to be dual bank partitioned

**Flash Partition**

- All but Cisco 7000 family, GSR, LS1010
  - partition flash 2 16 16
- Reversible mechanism
  - no partition flash
Use the Best Switching Path

- Available switching paths
  - Process switching
  - Fast switching
  - Cisco Express Forwarding (CEF)
    ```
    ip cef
    ```
- Router architecture and IOS internals
  RST-301

Fast Switching vs. CEF

Fast Cache Switching Scheme
- First packet sent to process level
- Subsequent packets switched at interrupt level using fast switching cache
- Cache is aged periodically causing packets to go to process level

CEF/Distributed CEF Switching Scheme
- No process switching
- All packets switched at interrupt level
- No cache aging
Agenda

- Basic Commands
- Network Management
- Administration
- Security
- Summary

Network Management
SNMP

- A very critical utility for network engineer
- An agent/manager model
- Circuits load, packets lost, router memory

Don’t Enable SNMP If You Aren’t Going to Use It As It Opens up Another Access Point to the Device

Enable SNMP

- Put in both community and contact names
- Don’t use obvious read/write strings
- Strongly protect the access: Views, access from outside our network
- Log the authentication failures
SNMP Configuration

- A basic secured configuration
  
  ```
  snmp-server community mywrite RW
  snmp-server community myread view myview RO 45
  snmp-server contact TAC (1 800 553 2447)
  snmp-server view myview mib-2 include
  access-list 45 permit 215.17.34.1
  access-list 45 deny any
  ```

SNMP Traps

- Routers can let you know when things go wrong
  
  ```
  snmp-server enable traps
  snmp-server enable traps snmp authentication
  ```

- Don’t forget—Set the trap source as a loopback interface
  
  ```
  snmp-server source loopback0
  ```

- Don’t enable if you aren’t using SNMP—Wastes CPU
MRTG

- Multi-router traffic grapher (multi-platform, free)
- Generate HTML pages showing the traffic load on network links
- http://www.mrtg.org

Graphing an Interface

Traffic Analysis for Ethernet4/0
System: mrt.cisco.com in Interface Ethernet4/0 (5)

Max In: 718 kB/s (7.18%)
Average In: 215 kB/s (2.15%)
Current In: 200 kB/s (2.00%)
Limit Console Interrupts

- Turn off debug out to the console port
  logging console alerts
- Use ‘logging buffered’ and set appropriate buffer size
  logging buffered 64000 debugging
- Debug is not sent to the console port providing the least risk to the router when using debug

Timestamp the Output

- Correlating debug output is difficult without synced timestamps between routers
  service timestamps log datetime localtime msec
  service timestamps debug uptime
Syslog Server

• Send day to day messages to a syslog server so you have a message history
  logging 1.2.3.4

• Use a loopback IP address for logging so all records have the same IP address
  logging source Loopback0

Log Files

• What do you do with the logs?
• Do you check them?
  Daily, weekly, monthly, at all?
• What do you do if you see errors/security breaches?
  What does your policy say?
Agenda

- Basic Commands
- Network Management
- Administration
- Security
- Summary
Policy

- Policy is a human decision process based on
  - Control vs. flexibility
  - Stability vs. potential chaos
  - Upfront cost vs. later cost
- Usually involves a level of compromise

Policy—What Should It Cover?

- Security
  - Device access
  - Physical access
  - Counter measures
- Internet usage
- Upgrade procedures
  - IOS versions, etc.
- Moves, adds, and changes
- Disaster recovery
Authenticate Users

- Need to decide privilege hierarchy
- Need to decide authorization strategy
  - Generic or per user
  - AAA via TACACS+ or RADIUS
  - Local authentication

Local User Authentication

- Give each user a password
  
  aaa new-model
  aaa authentication login neteng local
  username joe password 7 1104181051B1
  username jim password 7 0317B21895FE
  line vty 0 4
  login authentication neteng
Distributed User Authentication

- Use a server-based distributed authentication system such as:
  - RADIUS
  - TACACS+

```
  aaa new-model
  aaa authentication login default tacacs+ enable
  aaa authentication enable default tacacs+ enable
  aaa accounting exec start-stop tacacs+
  ip tacacs source-interface Loopback0
  tacacs-server host 215.17.1.1
  tacacs-server key CKr3t#
```

Limit Authority

- Differentiate users authority on the router
  - Help desk
  - Operations
  - Second level/third level support

- Use privilege levels (0–15)
Set Privileges

- Set level of privilege for each user class
  
  ```
  username gltest privilege 5 password 0 gltest
  privilege configure level 5 interface
  privilege interface level 5 shutdown
  privilege exec level 5 show ip route
  privilege exec level 5 configure terminal
  privilege exec level 5 show running-config
  ```

Backup Your Configurations

- Sounds obvious…
- Do you do it?
- Do you do it regularly?
- Do you keep a change history?
**Configuration Management**

- Backup NVRAM configuration of the router:
  - Write configuration to TFTP server
  - TFTP server files kept under revision control
  - Router configuration built from master database
- Allow rapid recovery in case of emergency

**Out of Band Management**

- Allows access to network equipment in times of failure
- Ensure quality of service
  - Minimise downtime
  - Minimize repair time
  - Ease diagnostic and debugging
Set up Dial-in for the TAC

- If your policy allows for remote support (dial up), set it up
- Use a modem on the console
- More importantly test it every so often
- When something is broken, it's not the time to set up a connection
- To maintain security leave the modem powered off until it is needed

Agenda

- Basic Commands
- Network Management
- Administration
- Security
- Summary
Security

Our Playground

Enterprise — CPE — Provider

DMZ — Internet
Turning Global Services OFF

- Turn off extra services (echo, discard, etc.)
  - no tcp-small-servers
  - no udp-small servers
  - no service pad
  - no ip bootp server
  - no service finger

Turning Services OFF

- Remove telnet access where possible on physical and virtual interfaces
  - transport input ‘keyword’
  - transport output ‘keyword’
  - transport preferred ‘keyword’
- Remove services on interfaces
  - no ip redirects
  - no ip proxy-arp
  - no ip directed-broadcast
Password Encryption

- For local authentication use password encryption
  Encryption '7' on a Cisco is reversible
  The “enable secret” password encrypted via a one way algorithm
  service password-encryption
  enable secret mysecret

Passwords Policy

- Use strong passwords
  Have a policy of minimum length, use special characters, etc
  Use `cisco`/`cisco` for testing only; Don’t use it in a production environment
- Change your passwords on a regular basis
  This is easier if using TACACS+/RADIUS
VTY and Console Port Timeouts

- Default idle timeout on async ports is 10 minutes 0 seconds
  
  `exec-timeout 10 0`

- TCP keepalives on incoming network connections
  
  `service tcp-keepalives-in`

VTY Security

- Access to VTYs should be controlled,
- Consoles should be used for last resort admin only

```
line vty 0 4
access-class 3 in
exec-timeout 5 0
transport input telnet ssh
transport output none
transport preferred none
password 7 045802150C2E
access-list 3 permit 215.17.1.0 0.0.0.255
access-list 3 deny any
```
VTY Access-List

- Use robust ACLs with the logging feature to spot the probes on your network
  
  access-list 199 permit tcp 215.17.1.0 0.0.0.255 any
  access-list 199 deny tcp any any range 0 65535 log
  access-list 199 deny ip any any log

Verify Sources

- Limits the possibility of hacks by unauthorised users/devices
- This is available for items such as:
  
  Routing information—EIGRP, BGP, OSPF
  NTP sources
  SNMP servers
  TFTP servers
- Achieved using basic password or MD5 hashed passwords
Unicast Reverse Path Forwarding

- **Unicast**
- Source IP packets checked to verify route back to the source uses the same interface
- If the packet does not arrive on the RPF interface, the packet is silently discarded
- CEF switching must be enabled

CEF Unicast RPF

Routing Table:
- 210.210.0.0 via 172.19.66.7
- 172.19.0.0

CEF Table:
- 210.210.0.0 172.19.66.7 Fa 2/0/0
- 172.19.0.0

Adjacency Table:
- Fa 2/0 172.19.66.7 0055FAC1801 00055FAF2C060800

Data IP Header

Dest Addr: x.x.x.x
Src Addr: 210.210.1.1

RPF Checks to See If the Source Address’s Reverse Path Matches the Input Port

If OK, RPF Passed the Packet to Be Forwarded by CEF

Copyright © 1999, Cisco Systems, Inc. All rights reserved.
CEF Unicast RPF

Routing Table:
- 210.210.0.0 via 172.19.66.7
- 172.19.0.0 is directly connected, Fa 2/0/0

CEF Table:
- 210.210.0.0 172.19.66.7 Fa 2/0/0
- 172.19.0.0 attached Fa 2/0/0

Adjacency Table:
- Fa 2/0/0 172.19.66.7 00055FAC1801 00055FAF2C0600

RPF Checks to See If the Source Address’s Reverse Path Matches the Input Port

If Not OK, RPF Drops the Packet

Unicast RPF

Packet Filtering

Deny Source Address 165.21.1.0/24

Allow Source Address 165.21.1.0/24
Filtering Configuration

• Interface Serial0 configuration
  
  interface serial0
  ip access-group 150 in
  ip access-group 160 out

  access-list 150 deny ip 165.21.1.0 0.0.0.255 any
  access-list 150 permit ip any any
  access-list 160 permit ip 165.21.1.0 0.0.0.255 any
  access-list 160 deny ip any any

Reflexive Access List

• Created when an outgoing session is initiated
• Deleted when the session stops
  (FIN, RST, timer)
• Valid for TCP, UDP, ICMP, etc
Reflexive Access-list Configuration

- **Reflect**
- **CPE**
- **Provider**

```plaintext
ip access-list extended outboundfilters
permit tcp any any reflect tcptraffic
ip access-list extended inboundfilters
evaluate tcptraffic
```

Rate Limiting

- **How much ICMP traffic is it sensible to receive?**
  - How do you stop your bandwidth to be wasted?
  - **Answer:** Rate limit the bad traffic
- **Committed Access Rate (CAR)**
Implementing Rate Limiting

- Layer-3 input and output limits
- Aggregate and granular limits
  - Port, MAC address, IP address, application

Rate Limiting Example

- Limiting ICMP traffic to 256 kbps
  - Traffic we want to limit
    - access-list 102 permit icmp any any echo
    - access-list 102 permit icmp any any echo-reply
  - Interface configuration for border
    - interface Serial0
    - rate-limit input access-group 102 256000 8000
      8000 conform-action transmit exceed-action drop
Agenda

- Basic Commands
- Network Management
- Administration
- Security
- Summary

Summary
Call to Action

• Have a network policy
• Configure basic IOS features
• Set up management features
• Secure your network

Questions?
Useful Links

- Supporting IOS Essentials White Paper

- Feature Navigator

- Connecting a Modem to the Console Port

- Best Practices

IOS Configurations…
What Should Be in Them,
but Sometimes Isn’t!

RST-204
Please Complete Your Evaluation Form

RST-204