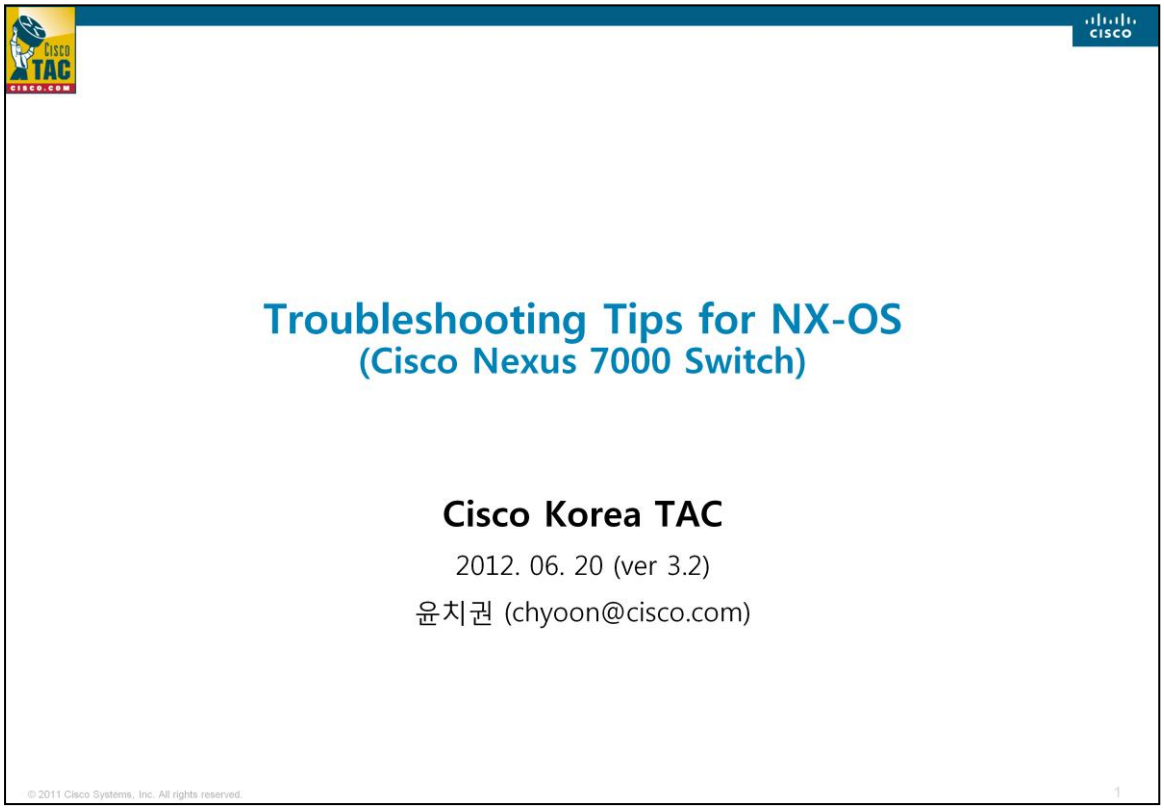


시스코 서비스 뉴스레터 2012년 6월호의 기술문서는, 지난 4월호 뉴스레터 피드백을 통해서 고객/파트너 분들이 주신 의견을 반영하여 '시스코 Nexus 7000 스위치' 트러블슈팅으로 주제를 정했습니다.

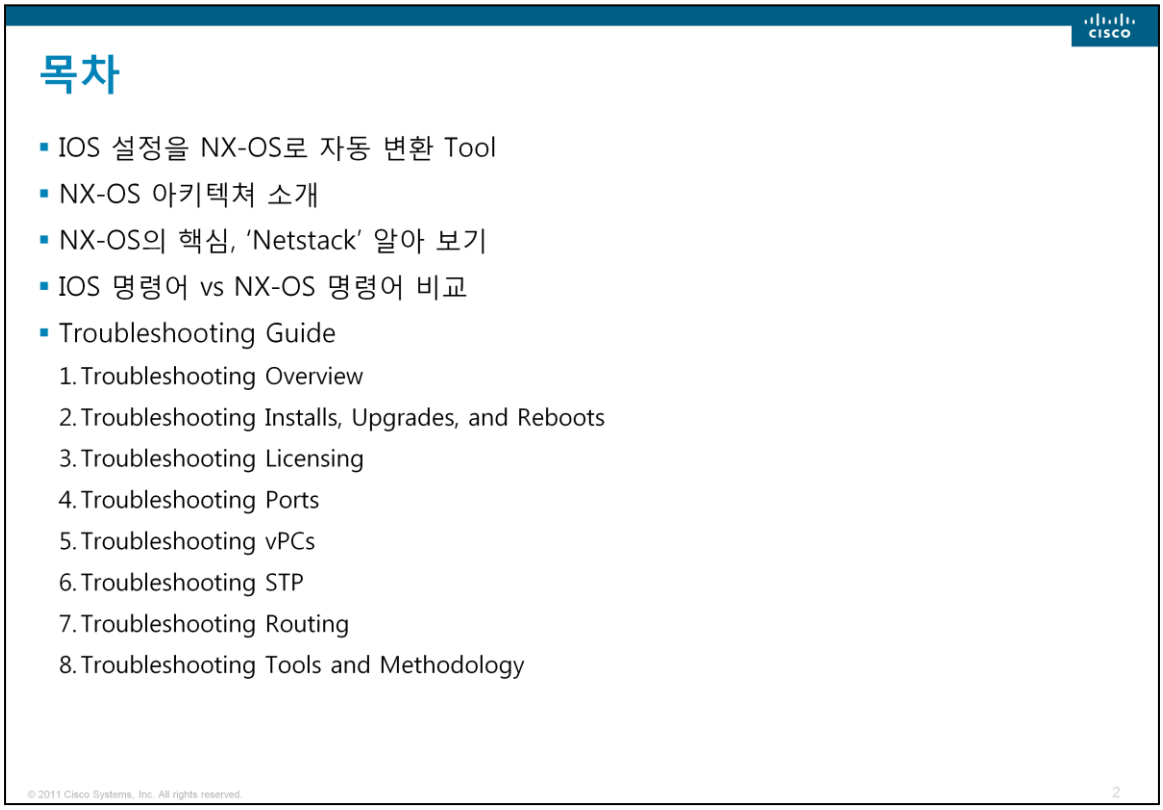
또한, 필드에서 많은 엔지니어 분들이 시스코 Nexus 7000 스위치를 사용하시면서 궁금한 점이 있으셨을 것으로 판단되어 도움이 되고자 문서를 제작하였습니다. 그리고 Korea TAC에서 기술지원을 하면서 필요하다고 생각되는 기본적인 내용들도 같이 담았습니다.

TAC에 case가 열리는 내용 중 재미있는 사실은 Nexus 7000 스위치를 비롯한 NX-OS를 사용하는 Nexus 계열 스위치에서 열리는 케이스 중에는 장애와 직접 연관이 없는 부분에 대한 문의 즉, Nexus 플랫폼의 제약사항, 기존 Catalyst와 다른 기능, 동작방식에 대한 문의가 종종 있습니다. 이를 위해서 다른 플랫폼(카타리스트 IOS)과 다른 점에 대해서도 간략한 내용을 포함했습니다.

저희 Korea TAC에서 발행하는 기술문서가 모든 문제를 해결하기에는 부족하나, 적어도 모든 부분에 걸쳐서 최소한의 기본이 되는 정도의 정보를 드리기 위한 문서를 만들기 위해 노력했습니다. 또한 실제로 TAC case가 열린 것 중에서 다른 고객/파트너 분들도 동일한 질문 혹은 이슈가 될 수 있는 부분을 요약해서 중간 중간에 Tip 형태로 배치를 하였습니다.

참고로 'NX-OS'는 NeXt-generation' Operating System의 약자 입니다.

All contents are Copyright © 1992–2012 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



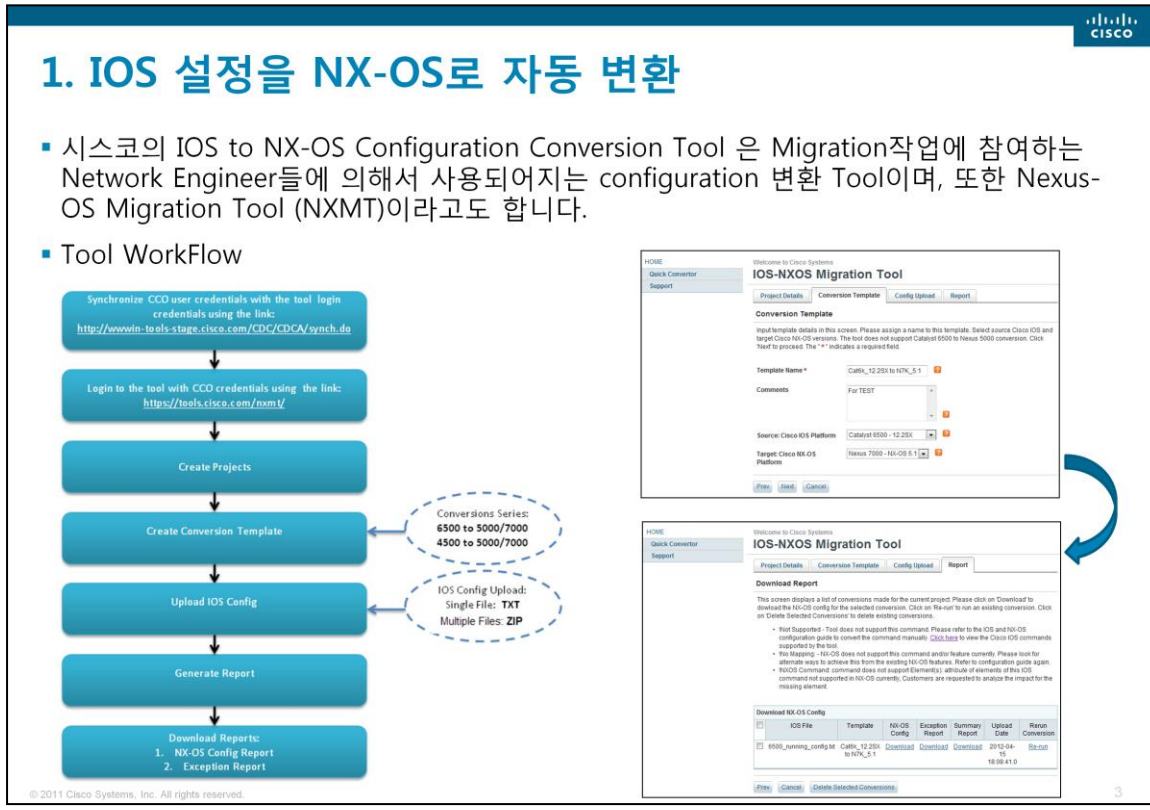
순서는 기존 Catalyst 6500 스위치를 Nexus 7000 스위치로 마이그레이션을 하는 단계부터 시작됩니다.

간단한 변한 Tool을 이용하여 Nexus 스위치로 마이그레이션을 잘 마치셨다면, NX-OS 소프트웨어 아키텍쳐를 이해할 필요가 있습니다. 그 중에서도 가장 핵심이 되는 'Netstack'에 대해서 살펴볼 것이고, 이해를 돕기 위해서 기존 IOS와의 명령어 차이점도 알아 보도록 하겠습니다.

마지막으로 트러블슈팅 측면에 대해서 각 영역별로 나눠서 기본적인 설명을 하겠습니다.
장비의 최초 설정, 라이센스, 소프트웨어 업그레이드 및 운영 중 발생할 수 있는 다양한 문제들...

또한 슬라이드 중간에는 원인분석을 위한 자료 수집의 Tip을 수록하여 이해를 돕기 위하여 노력하였습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



IOS to NX-OS Conversion Tool 이란?

시스코의 IOS to NX-OS Configuration Conversion Tool 은 Migration작업에 참여하는 Network Engineer들에 의해서 사용되어지는 configuration 변환 Tool이며, 또한 Nexus-OS Migration Tool (NXMT)이라고도 합니다.

이 툴은 IOS의 command나 configuration을 그에 상응하는 NX-OS의 값으로 변환하는데 사용됩니다. 이 툴의 사용자는 하나의 txt 형식의 파일 또는 Zip 형식의 여러파일을 업로드 하여 사용할 수 있으며, 결과값으로 변환된 NX-OS configuration 파일과 exception 파일 즉 Error report 파일을 download 할 수 있습니다.

특별히Quick Convertor Option은 사용자가 IOS 구문을 수동으로 입력하고 즉시 NX-OS의 값으로 변환시켜 간편하게 결과를 확인 할 수 있도록 도와줍니다.

IOS to NX-OS Conversion Tool URL

1) Main page

- http://tools.cisco.com/nxmt/

2) Support page

- http://tools.cisco.com/nxmt/scope.htm

Conversion가능한 IOS versions

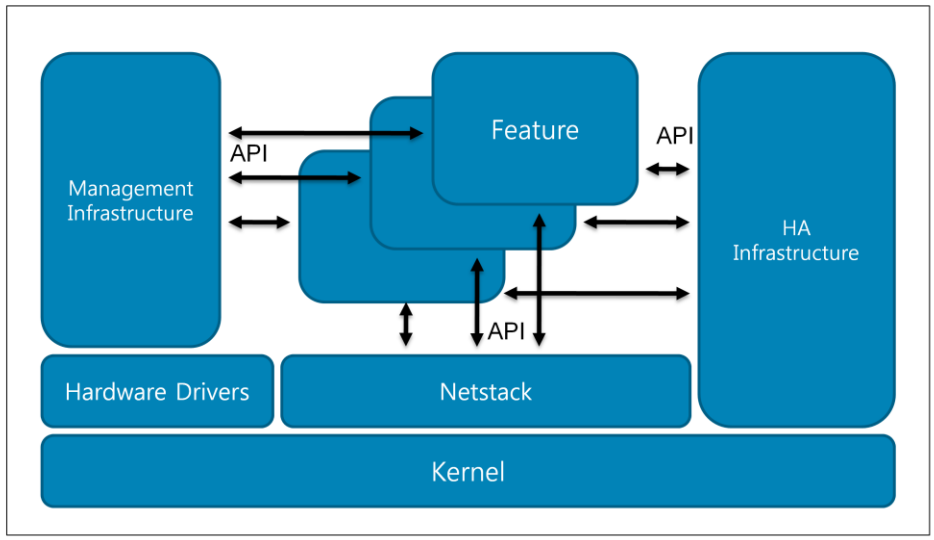
이 IOS to NX-OS Conversion Tool에서는 다음과 같은 version을 지원하고 있습니다.

참고로, 시스코 서비스 뉴스레터 2012년 4월호를 보시면,
Korea TAC 김민경 엔지니어가 작성한 아래 문서를 참고하시면 자세한 사용방법이 나와 있으니 참고해 주세요
http://www.cisco.com/web/KR/Service_Newsletter/2012/PDF/2012_04_2.IOStoNX_OS_Conversion_Tool.pdf

IOS	NXOS
6500	7000 (4.2, 5.0, 5.1 versions)
6500	5000 (4.2, 5.0, 5.1 versions)
4500	5000 (4.2, 5.0, 5.1 versions)
4500	7000 (4.2, 5.0, 5.1 versions)

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

2. NX-OS 아키텍쳐는 무엇이 다른가?



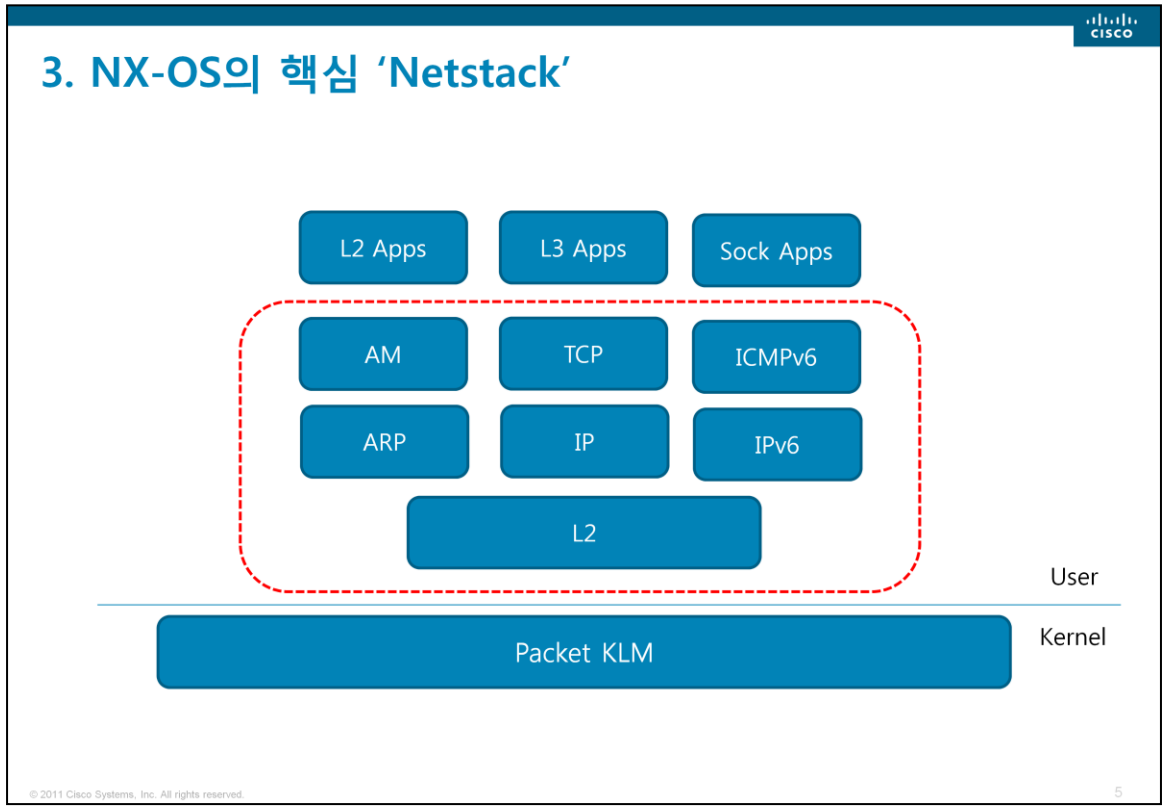
© 2011 Cisco Systems, Inc. All rights reserved.

전통적인 IOS 와 NX-OS는 Software Modularity라는 측면에서 차이가 있습니다.
NX-OX 소프트웨어의 이해가 Nexus 스위치를 이해하는 중요한 열쇠가 됩니다.

-Nexus7000 은 'self-contained network'(독립된 네트워크) 구조입니다.
-분리된 소프트웨어 컴포넌트들이 unicast 와 multicast를 이용하여 상호 작용을 하게 됩니다.
-Feature들은 persistence storage 및 message queue와 함께 MTS(Message Transport Service)를 활용합니다.
커뮤니이션들 사이에는 inspection tool이 배치되어 있습니다.
-Feature의 상태, feature 통신 그리고 queue를 지속적으로 review 합니다.

또한 Linux 기반임으로 가능한 잇점들, 예를 들어 멀태태스킹, 멀티쓰레드, 멀티코어, 멀티CPU 등을 가져올 수 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



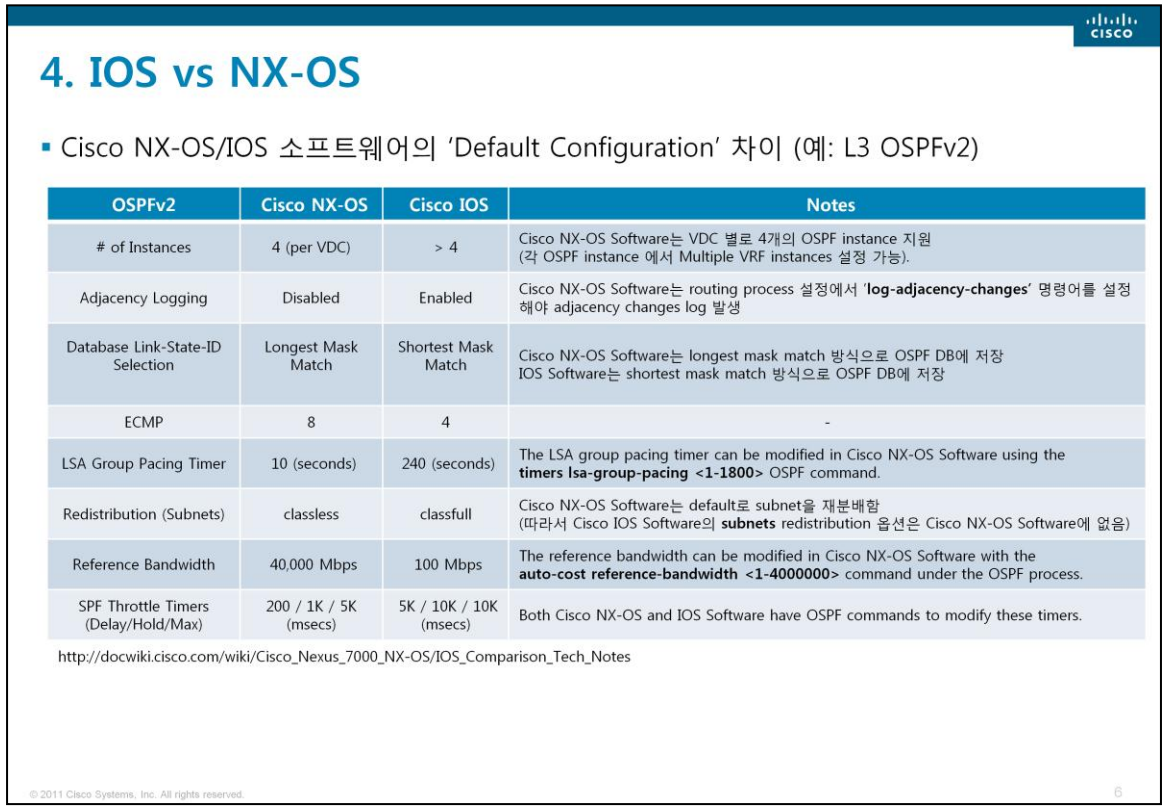
Netstack은 Supervisor Engine 위에서 동작하는 다음과 같은 'IP stack components'를 일컫는 용어로 사용되어 집니다.

Packet Manger, IPv4, ICMPv4, TCP/UDP, ARP, Adjacency Manager, IPv6, ICMPv6

추가적인 기능으로 Virtualization (VDCs/VRFs), High-Availability (SSO) 등이 있으며 이는 User 영역 안에 구현 되었습니다.

위의 표에서 보여지는 것처럼 Netstack은 각각 다른 components들로 구성됩니다.
Netstack 프로세스는 Packet Manager, IPv4, ICMPv4, 그리고 TCP/UDP로 이루어 집니다.
ARP, AM, IPv6, ICMPv6는 별도의 독립적인 프로세스들 입니다.
이런 프로세스들은 multi-thread 되어 지고, user space에서 구동됩니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



4. IOS vs NX-OS

- Cisco NX-OS/IOS 소프트웨어의 'Default Configuration' 차이 (예: L3 OSPFv2)

OSPFv2	Cisco NX-OS	Cisco IOS	Notes
# of Instances	4 (per VDC)	> 4	Cisco NX-OS Software는 VDC 별로 4개의 OSPF instance 지원 (각 OSPF instance 에서 Multiple VRF instances 설정 가능).
Adjacency Logging	Disabled	Enabled	Cisco NX-OS Software는 routing process 설정에서 '**log-adjacency-changes**' 명령어를 설정해야 adjacency changes log 발생
Database Link-State-ID Selection	Longest Mask Match	Shortest Mask Match	Cisco NX-OS Software는 longest mask match 방식으로 OSPF DB에 저장 IOS Software는 shortest mask match 방식으로 OSPF DB에 저장
ECMP	8	4	-
LSA Group Pacing Timer	10 (seconds)	240 (seconds)	The LSA group pacing timer can be modified in Cisco NX-OS Software using the **timers lsa-group-pacing <1-1800>** OSPF command.
Redistribution (Subnets)	classless	classfull	Cisco NX-OS Software는 default로 subnet을 재분배함 (따라서 Cisco IOS Software의 **subnets** redistribution 옵션은 Cisco NX-OS Software에 없음)
Reference Bandwidth	40,000 Mbps	100 Mbps	The reference bandwidth can be modified in Cisco NX-OS Software with the **auto-cost reference-bandwidth <1-4000000>** command under the OSPF process.
SPF Throttle Timers (Delay/Hold/Max)	200 / 1K / 5K (msecs)	5K / 10K / 10K (msecs)	Both Cisco NX-OS and IOS Software have OSPF commands to modify these timers.

http://docwiki.cisco.com/wiki/Cisco_Nexus_7000_NX-OS/IOS_Comparison_Tech_Notes

© 2011 Cisco Systems, Inc. All rights reserved.

기존 Catalyst 6500과 Nexus 간의 명령어 차이를 보시려면 아래 URL을 참고 하세요.
http://docwiki.cisco.com/wiki/Cisco_NX-OS/IOS_Software_Default_Configuration_Differences

각 기능에 따라서 IOS와 NX-OS 간 차이를 확인 하실 수 있습니다.

위 슬라이드는 한 예로써,
L3 OSPFv2 와 연관된 기능, 성능, 옵션, 기본값 등이 각각 어떻게 다른지를 확인 하실 수 있습니다.

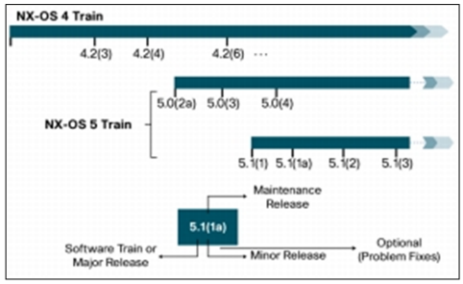
All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

Tip. NX-OS recommendation

- NX-OS Software Release 전략
  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps9494/ps9372/guide_c07-658595.html

- NX-OS 권고
  http://www.cisco.com/en/US/docs/switches/datacenter/sw/nx-os/recommended_releases/recommended_nx-os_releases.html

- NX-OS Software Release



© 2011 Cisco Systems, Inc. All rights reserved.

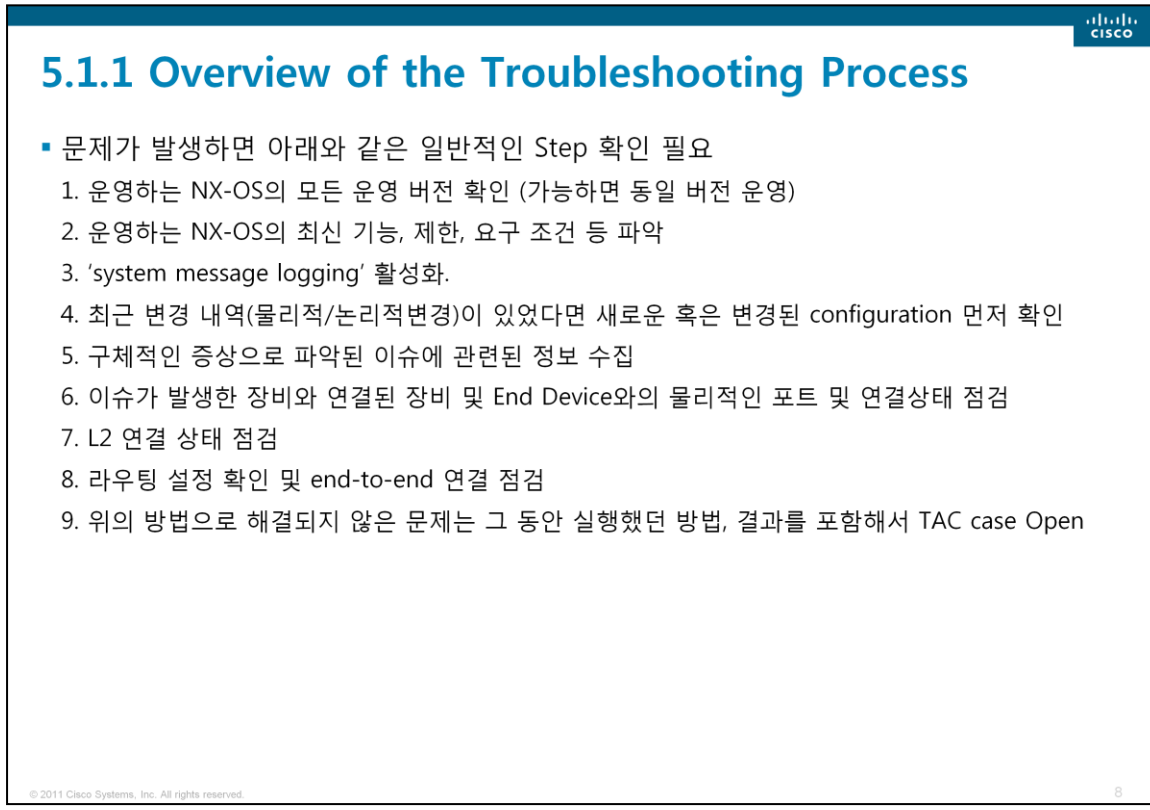
Case를 진행하면서 특정 Bug에 해당되면 TAC에서는 해당 버그가 Fixed 된 버전 및 상위 버전으로 업그레이드를 권고 하고 있습니다.

이 권고는 특정한 이슈에 해당되는 버그를 해결하기 위한 목적이지 각 고객 분들이 사용하시는 기능에 대해 이슈가 없음을 뜻하는 것은 아닙니다. 따라서 현재 사용하는 feature, 소프트웨어, 하드웨어 정보를 가지고 CCO를 통해서 OS를 선택 하시는 것이 좋습니다.

다만, 시스코 Nexus 담당하는 부서에서는 주기적으로 권고하는 버전을 CCO에 올려 놓고 권고를 합니다. 혹시라도 어떤 버전을 사용해야 할지 한번이라도 고민을 하셨다면, 주기적으로 위 홈페이지를 방문 하셔서 시스코에서 권고하는 버전을 확인 하실 수 있습니다.

또한 NX-OS가 어떤 전략을 가지고 만들어지고 EoS가 되는지에 대한 정보도 동시에 확인 하실 수 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



Chapter 5에서는 troubleshooting에 대한 내용으로 기본적인 프로세서부터 시작해서 TAC case를 Open하기 전에 수집해야 할 output에 대해서는 기술하였습니다.

NX-OS release note는 아래 URL에서 확인 가능 합니다.
http://www.cisco.com/en/US/products/ps9372/prod_release_notes_list.html
System message logging은 아래 URL에서 확인 가능 합니다.
http://www.cisco.com/en/US/docs/switches/datacenter/sw/system_messages/reference/sl_nxos_book.html

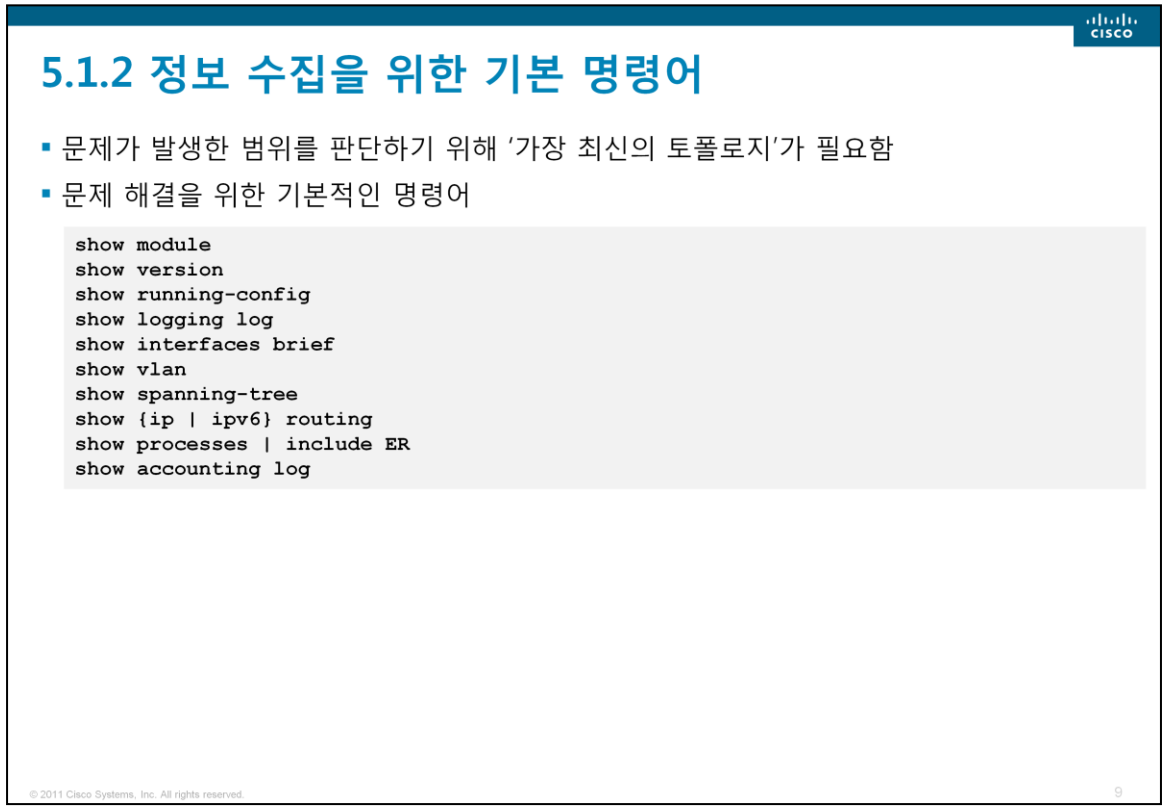
구체적인 증상으로 정의되면 관련된 명령어를 통하여 정보를 수집합니다.
예) 기본적인 장치 정보(H/W, S/W, Feature), Port 정보, L2 연결정보, STP 관련정보, L3 연동정보, 라우팅 정보
기본적인 Tool (Ping, Trace, etc)를 이용한 간단한 테스트 및 관련 정보 수집

물리적인 포트 연결 상태 확인
1) 연결 미디어 상태 확인 (copper, optical, fiber type)
2) 미디어의 연결상태가 끊어졌는지, 피해를 입었는지?
3) 포트 및 모듈의 LED 상태가 green으로 올바르게 점등 되어 있는지?
4) VDC를 사용하는 환경이라면 각 인터페이스가 각 VDC에 올바르게 할당되어 있는지? (vdc membership)
5) 각 인터페이스의 운영상태가 올바른지? (show interface brief)

L2 연결 상태 확인에 도움이 되는 명령어
show vlan all-ports : 필요한 인터페이스들이 동일 vlan에 잘 설정되어 있는지 확인
show port-channel : 포트채널 그룹에 속한 포트들이 동일한 seed, duplex, trunk mode로 설정
show running-config spanning-tree : 연동장비에 동일한 Spanning Tree Protocol이 설정되어 있는지 확인
show processes | include ER : 중요한 Layer 2 프로세스가 error 상태에 있는지 확인 하기
show spanning-tree blockedports : STP에 의해서 block된 포트 확인
show mac address-table dynamic vlan : 각 node에 대한 learning 상태 및 aging 상태 확인

L3 연결 상태 확인
1) Default gateway는 올바르게 설정 되어 있는가?
2) 동일한 dynamic routing protocol이 구동되는 domain 내에 동일한 parameter로 설정 되어 있는가?
3) 문제가 되는 경로에 대한 Access List, route map 혹은 라우팅 업데이트를 반행하는 설정이 있는가?

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Confidential

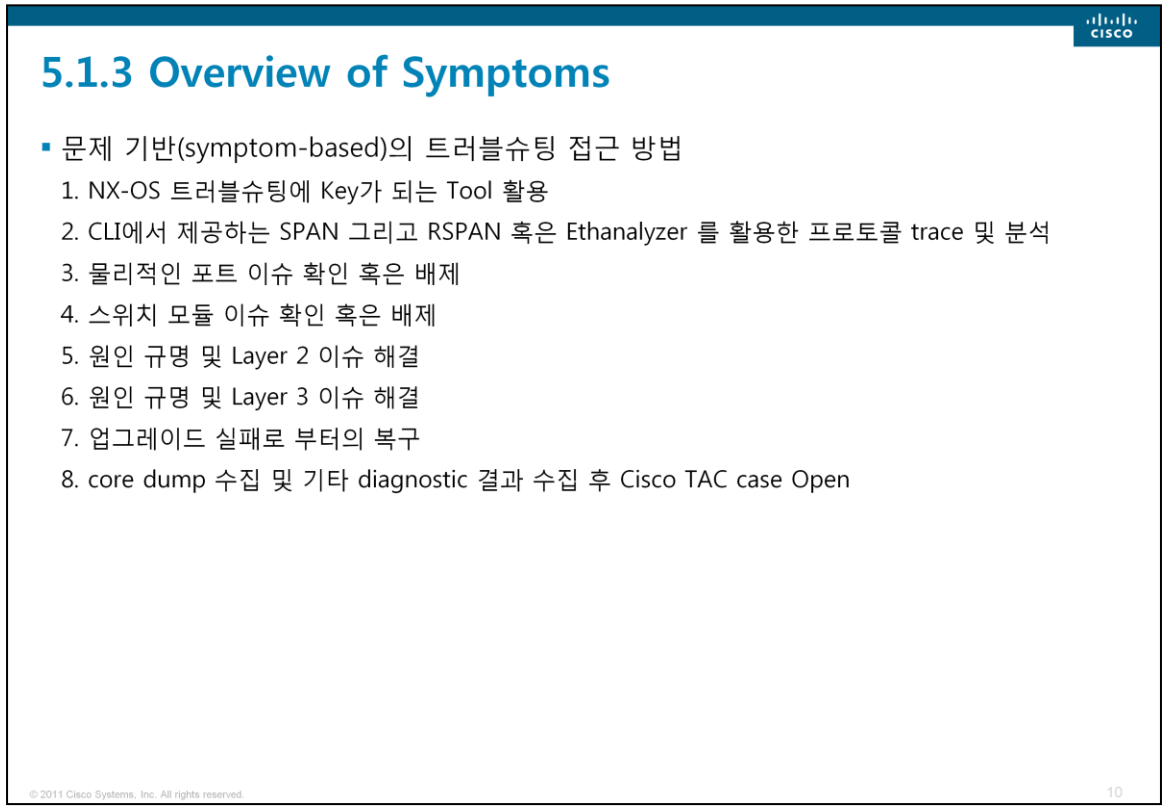


망에서 발생한 문제를 트러블슈팅 혹은 정보 수집을 하기 위해 필요한 가장 기본적인 명령어가 될 것 입니다.

위의 명령어들은 특정 문제를 해결하기 위함이 아니라 문제가 발생한 하드웨어, 소프트웨어 버전을 우선확인하고, 특정 설정(config) 및 최근에 발생한 logging 그리고 process 확인과 더불어 최근 수행되었던 명령어 들을 보는 것으로 부터 시작 됩니다.

망을 잘 이해하고 있는 사람이라도 네트워크 다이어그램을 펼쳐 놓고 각 장비에서 발생한 이벤트를 위주로 보면서 이슈를 좁혀나가는 과정이 필요하게 됩니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



증상기반(symptom-based) 문제해결 접근은 다음 각 슬라이드에서 설명드린 것처럼 문제를 특정 영역 혹은 기능으로 분류해서 NX-OS에 발생한 문제를 진단하고 해결할 수 있도록 도움을 줄 수 있게 됩니다.

장비간에 운영되는 많은 프로토콜에 의해서 많은 정보를 가지고 있는 장비에서 문제가 발생함으로써 문제가 발생한 장비 혹은 특정 기능을 찾아 낸다는 것은 어려운 일이 될 수 있으나, 이렇게 특정 증상을 기반한 narrow-down 방법으로 문제를 접근하고 풀어 나간다면 문제는 '한 문장' 혹은 '하나의 keyword'로 요약할 수 있게 되고, CCO를 통한 검색 혹은 TAC을 통한 기술지원을 받을 때에도 큰 도움이 됩니다.

이런 문제들과 문제해결을 위한 action에는 다음과 같은 것들이 수반되어 집니다.

-문제 해결을 위해 핵심이 되는 NX-OS troubleshooting tools

-NX-OS CLI에서 제공하는 SPAN 그리고 RSPAN 혹은 Ethanalyzer를 활용하여 Protocol 분석

-물리적 포트 이슈 확인 혹은 배제

-스위치 모듈 이슈 확인 혹은 배제

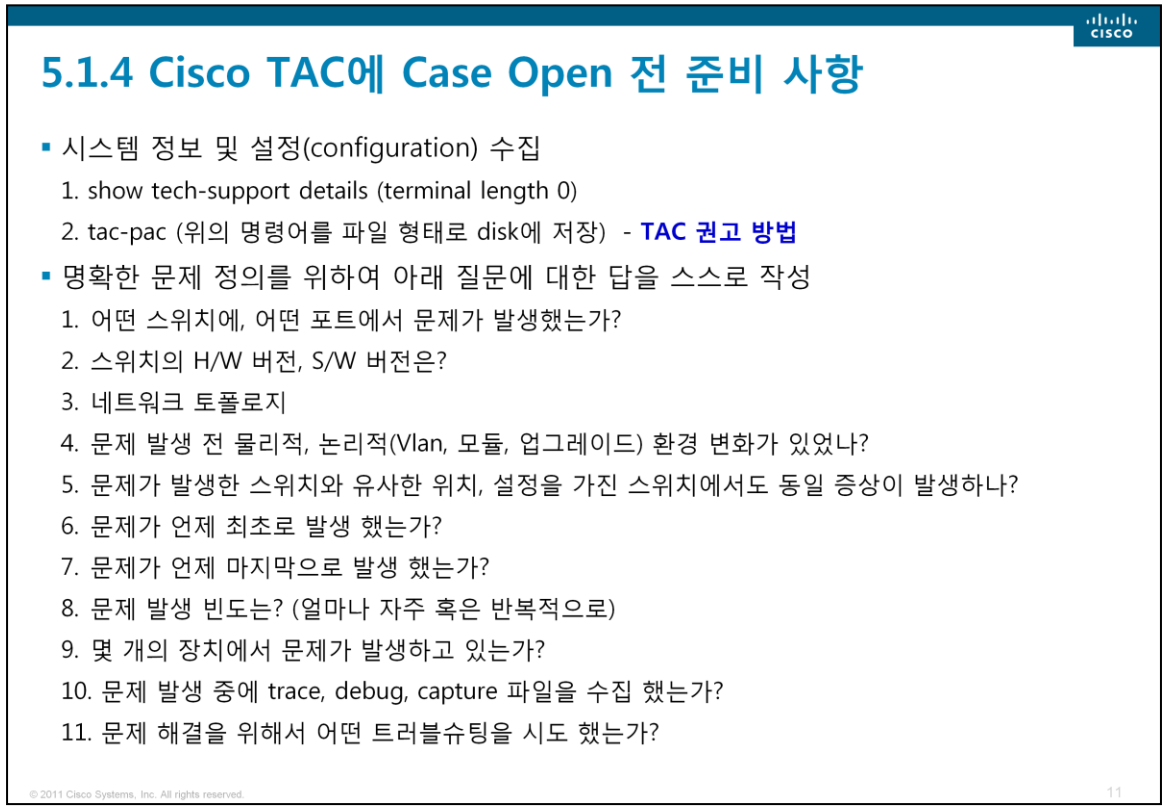
-Layer2 이슈 규명 혹은 정정

-Lyaer3 이슈 규명 혹은 정정

-스위치 업그레이드 실패로 부터의 복구

-TAC 지원을 받기 위해 필요한 core dump 혹은 다른 diagnostic 결과 수집

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



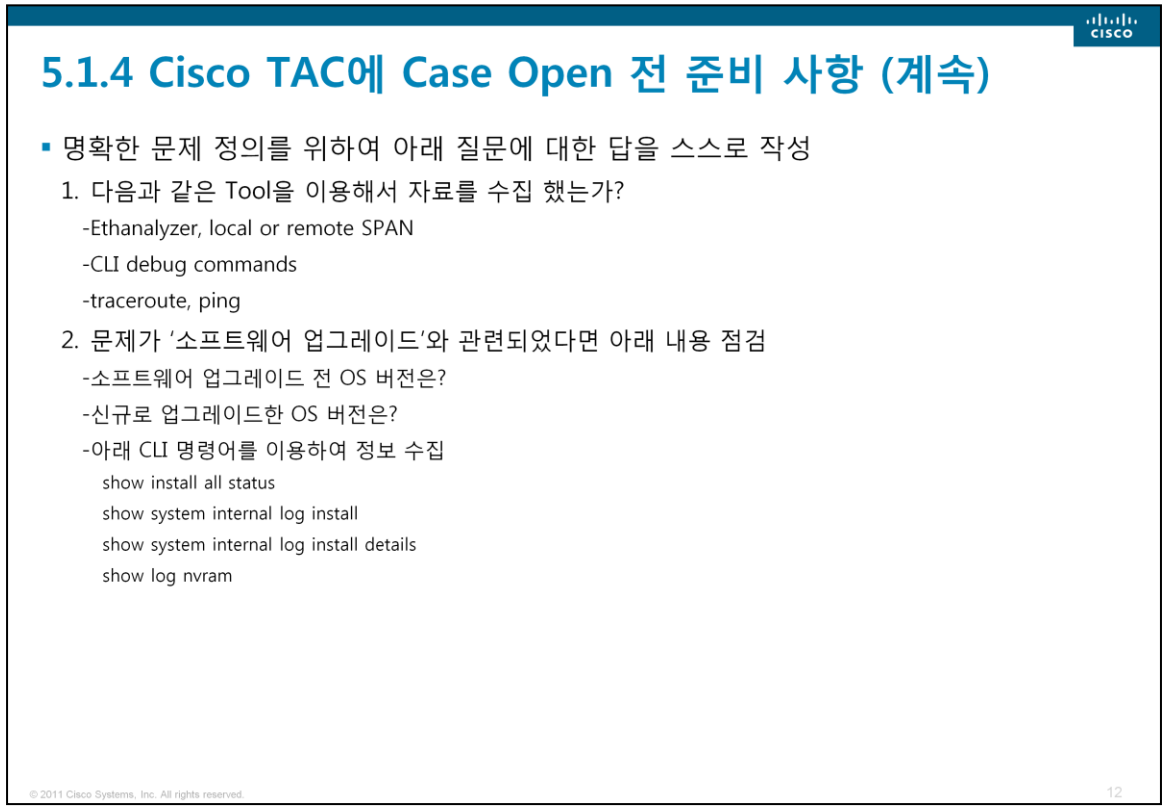
Cisco TAC과 함께 Case를 진행해 보셨다면, TAC 엔지니어로 부터 아래와 같은 내용의 이메일을 받은 적이 있으실 것입니다.

어떤 스위치에, 어떤 포트에서 문제가 발생했는가?
스위치의 H/W 버전, S/W 버전은?
네트워크 토폴로지
문제 발생 전 물리적, 논리적(Vlan, 모듈, 업그레이드) 환경 변화가 있었나?
문제가 발생한 스위치와 유사한 위치, 설정을 가진 스위치에서도 동일 증상이 발생하나?
문제가 언제 최초로 발생 했는가?
문제가 언제 마지막으로 발생 했는가?
문제 발생 빈도는? (얼마나 자주 혹은 반복적으로)
몇 개의 장치에서 문제가 발생하고 있는가?
문제 발생 중에 trace, debug, capture 파일을 수집 했는가?
문제 해결을 위해서 어떤 트러블슈팅을 시도 했는가?

실제 이런 질문들은 장애 내용과 크게 연관이 없어 보이나, 문제는 처음 접하는 TAC 엔지니어 한테는 문제는 올바로 인식하기 위해서 필요한 정보들입니다.

물론 실제 망을 운영하시는 분들은 해당 망에 대한 정보/지식/경험이 많음으로써 문제를 금방 이해하지만, 해당 네트워크에 대해서 처음 접한 TAC 엔지니어는 해당 문제를 다른 관계없는 이슈들과 해당 문제를 분리시키는 작업이 필요해 지고, 위의 기본적인 배경지식을 바탕으로 추가적으로 받아지는 결과물을 제대로 인식하고 판단하기 위해 위의 내용을 배경지식으로 활용한다는 점을 이해해 주시면 좋겠습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



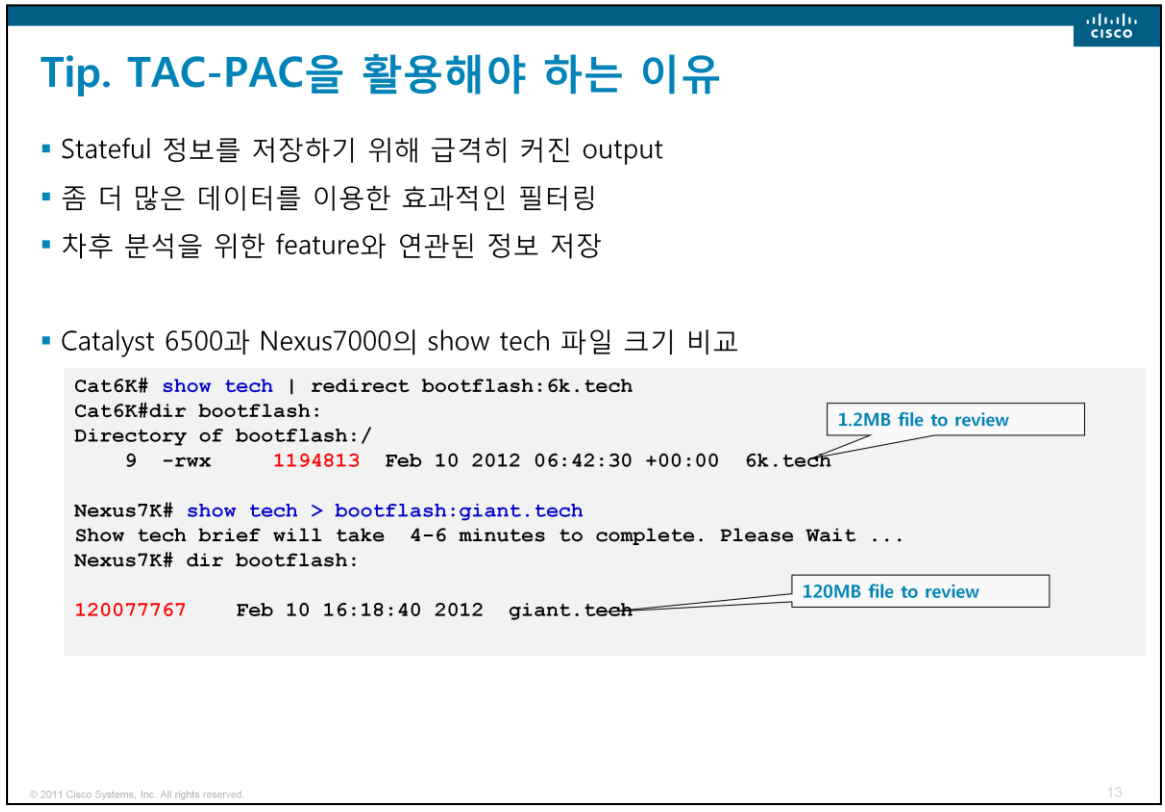
앞선 슬라이드에서도 설명을 드렸지만, 문제가 발생하게 되면 간단하게는 몇 개의 show 명령어로 문제를 확인하고 판단하는 경우도 있습니다.

그러나 대부분의 문제들은 추가적인 명령어로 몇 차례 받아서 결과물을 봐야 하는 경우도 있습니다.
또한 문제가 더 세밀하고 복잡한 경우에는 장비에서 수집하는 결과물 외에 NX-OS CLI에서 제공되는 tool을 활용하여 정보를 수집해야 하는 경우도 있습니다.

이런 경우에는 SPAN 그리고 RSPAN 기능을 이용하여 트래픽 분석기 (예, 와이어샤크)가 연결되어 있는 포트로 특정 트래픽을 복사해서 분석할 수 있도록 도움을 주게 됩니다.

더불어 CPU로 향하는 트래픽의 경우에는 NX-OS에 탑재된 Ethanalyzer를 활용하여 바로바로 트래픽을 수집하고 분석할 수 있는 기능을 제공하고 있습니다. 이런 경우에는 트래픽 분석기를 별도로 연결하지 않아도 된다는 장점이 있습니다. 자세한 활용방법은 뒤의 슬라이드를 참고해 주세요.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



위의 두 비교에서 알 수 있듯이, 기존 catalyst 6500에 비해서 Nexus7000 스위치의 show tech-support 크기가 증가 했습니다. 물론 증가한 크기만큼 더 많은 로그를 저장하고 있어서 왠만한 문제는 해당 파일을 통해서 분석이 가능하게 된 점도 있습니다.

장착된 모듈에 따라서 다소 시간차이가 발생하기는 하나 기본적으로 100Mb 정도 수집되므로 콘솔이나 텔렛을 통해서 show tech을 받는 다는 것은 무리가 있습니다.

따라서 위와 같이 기존에 사용하던 것처럼 'redirect' 옵션을 사용하여 show tech을 disk에 바로 저장하는 방법도 하나의 방법이 될 수 있습니다.

그러나 이 또한 파일 사이즈가 크므로 추가적인 방법이 추가 되었습니다.

다음 슬라이드에 나오는 **tac-pac** 명령어가 그것 입니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

Tip. TAC-PAC

- Compressed 'show tech'
- '**tac-pac**' 명령어를 이용하여 '압축된 show tech' 파일을 약 10MB 내외로 수집 가능

```
Nexus7K# tac-pac     // 명령어 수행 후 수 분 정도 소요 되므로 기다려야 함

Nexus7K# dir bootflash: | egrep show_tech
Nexus7K# copy bootflash:show_tech_out.gz ftp:

// 파일 생성이 완료 된 후 download 가능
```

- 사용 방법

  1. show tech-support details 결과를 redirect 하려 파일로 압축 저장하기 위해 tac-pac 명령어 이용

  2. 파일 이름을 지정하지 않으면, Cisco NX-OS는 volatile:show_tech_out.gz. 파일로 생성한다.

- 참고 문서

  1. http://www.cisco.com/en/US/partner/docs/switches/datacenter/sw/best_practices/cli_mgmt_guide/tac_data.html

  2. http://www.cisco.com/en/US/partner/docs/switches/datacenter/sw/6_x/nx-os/fundamentals/command/reference/fnd_commands.html#wp1471853

© 2011 Cisco Systems, Inc. All rights reserved.

tac-pac은 Nexus에서 사용할 수 있는 명령어로 'show tech-support detail' 결과를 disk에 압축하여 저장해 주는 명령어입니다. 특별히 파일명을 지정하지 않으면 show_tech_output.gz으로 저장이 됩니다.

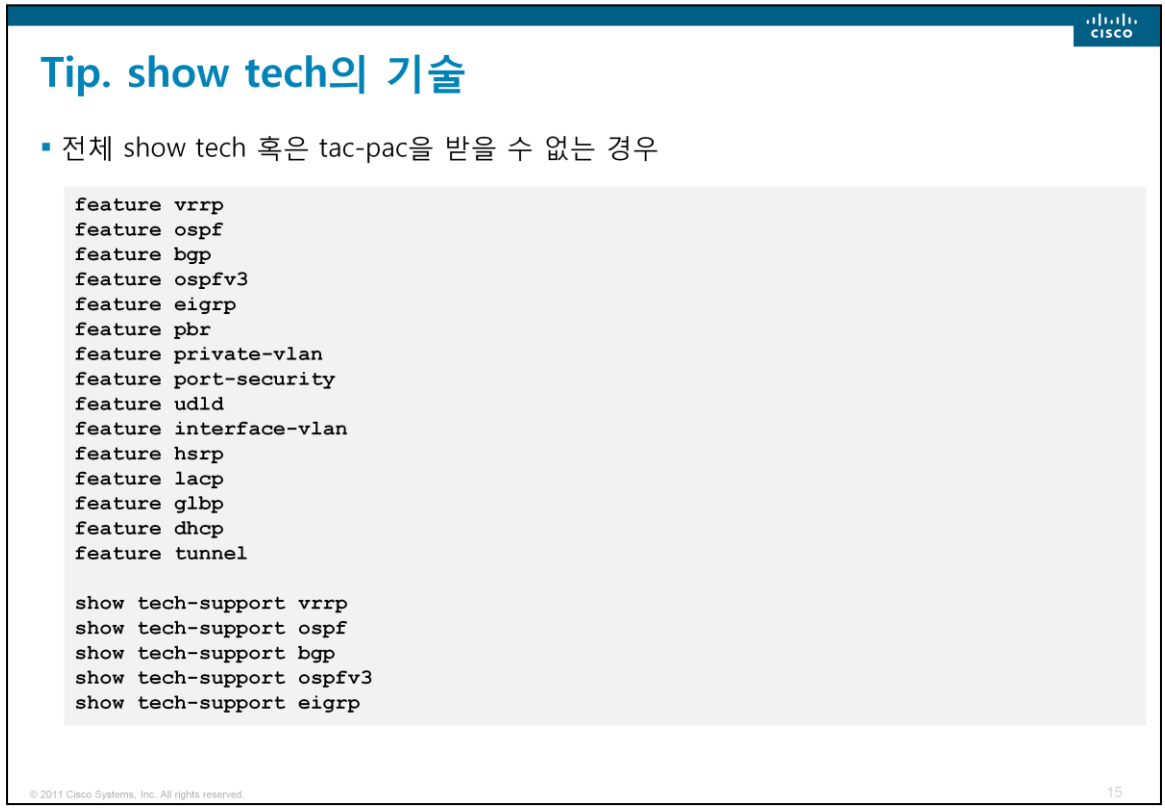
Disk에 저장된 '압축된 show tech'파일은 PC로 다운로드해서 풀어서 보실 수 있습니다.
혹시라도 사용하시는 nexus 장비에 이슈가 발생해서 TAC case를 Open 하시려고 show tech을 받아야 한다면 tac-pac 활용하시기 바랍니다.

구문
switch# tac-pac bootflash://showtech.switch1

명령어
tac-pac [bootflash: | ftp: | scp: | sftp: | slot0: | tftp: | volatile:]

bootflash: (Optional) Specifies the internal Flash memory.
ftp: (Optional) Uses FTP to download the file.
scp: (Optional) Uses Secure Copy Protocol (SCP) to download the file.
sftp: (Optional) Uses Secure Shell FTP (SFTP) to download the file.
slot0: (Optional) Specifies the external Flash memory.
tftp: (Optional) Uses Trivial FTP (TFTP) to download the file.
volatile: (Optional) Specifies the volatile memory on the device.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



앞장에서 보신 것처럼 Nexus 스위치의 show tech 사이즈가 크기 특정 문제를 이미 알고 있다면 특정 기능(feature)에 대해서만 show tech을 받아서 분석이 가능합니다.

물론 show tech에 포함되지 않은 정보를 위해서 별도로 특정 show tech을 받는 경우도 종종 있습니다.

더불어서 show tech을 받을 수 없거나 tac-pac을 받을 수 없는 상황에서 유용하게 활용 할 수 있습니다.

각 feature의 show tech은 위와 같이 각각 enable된 feature에 대해서 수집이 가능합니다.

show tech-support vrrp

show tech-support ospf

show tech-support bgp

show tech-support ospfv3

show tech-support eigrp

show tech-support details

'uptime', 'version', 'modules present', 'syslog' 등의 정보 포함

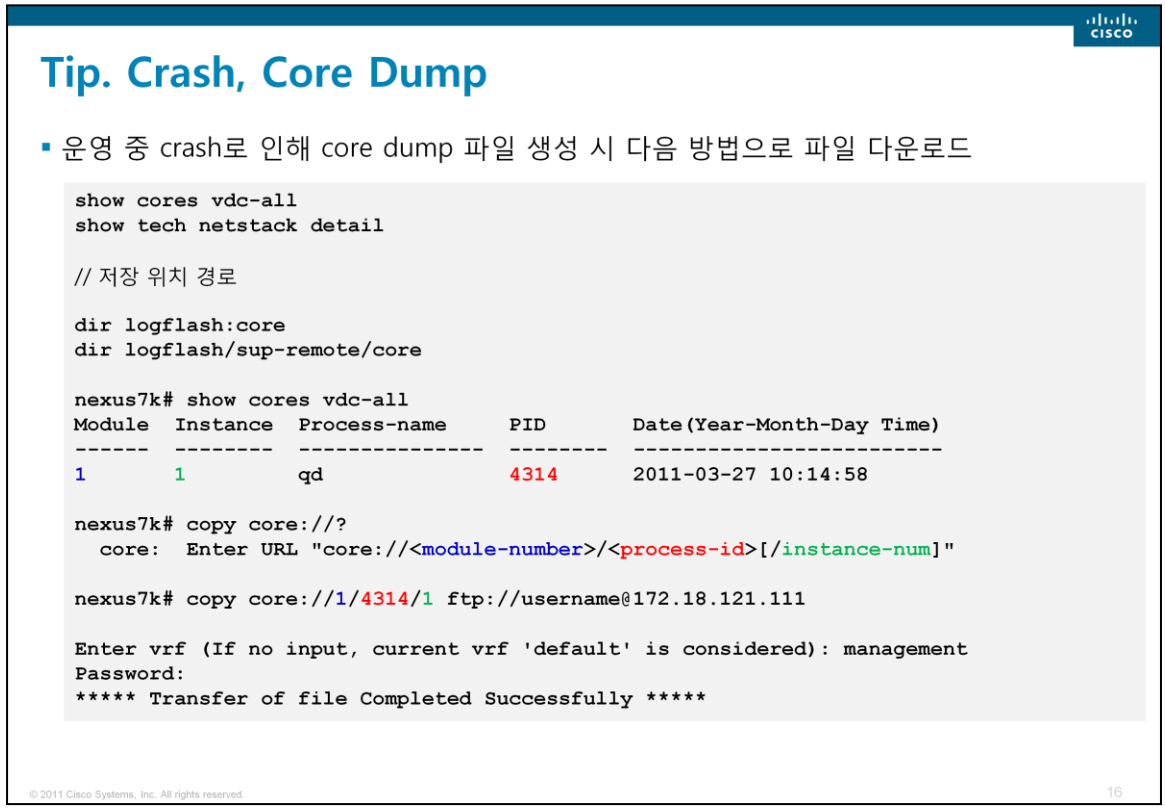
show tech-support platform :

supervisor (Linecard Manager, XbarManager, PlatformManager etc) 에서 구동되는 모든 플랫폼 레벨 컴포넌트에 대한 정보

show tech-support internal module <x> :

통계정보, 에러, 예외처리, reset reason 등 모듈과 연관된 특정한 정보

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



Core dump는 crash전에 system 과 software의 상세 정보를 포함하고 있는 덤프 파일입니다.
생성/저장된 덤프파일은 TFTP 서버를 이용하여 disk에 저장된 core dump 파일을 다운로드 받을 수 있습니다.
Cisco TAC case를 open하기 전 core dump 파일이 생성되었다면 해당 파일을 다운로드 받아서 보내 주세요.

위에 보시는 것처럼 저장된 core dump 파일을 보시려면,
show cores vdc-all 명령어를 통해서 보실 수 있습니다.

또한 standby engine에 저장된 core dump 파일도 아래와 같은 방법으로 확인 할 수 있습니다.
dir logflash/sup-remote/core

core dump 파일이 생성 되었다면 show core vdc-all 명령어를 통해서 Core가 저장된 모듈, PID, instance 번호를 확인하시고 copy 명령어를 이용하여 형식에 맞게 입력하시면 됩니다.
core: Enter URL "core://<module-number>/<process-id>[/instance-num]"

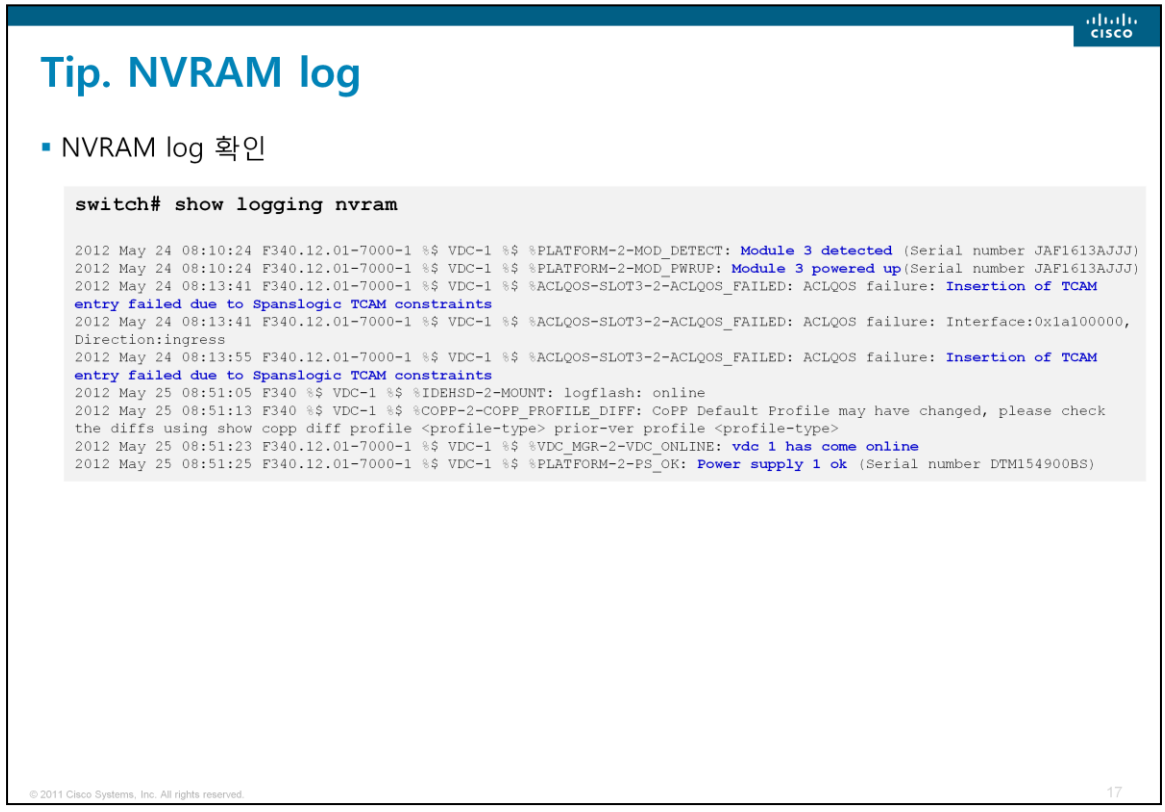
각 directory는 아래와 같이 다양하게 존재합니다.

show cores [vdc X]
logflash:/core/
logflash:/debug/
logflash:/log/
logflash:/generic/
logflash:/eem_logs/

switch# dir logflash:

```
   4096    Jan 07 06:52:25 2010  core/
   4096    Jan 07 06:52:25 2010  debug/
   4096    Mar 11 07:07:46 2012  eem_logs/
  59022    Jun 01 04:00:19 2012  event_archive_1
  50025    Jun 06 12:20:24 2012  fpm_cplog.9
   4096    Jan 07 06:52:25 2010  generic/
   4096    Jan 07 06:52:25 2010  log/
  16384    Jan 07 06:50:40 2010  lost+found/
```

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



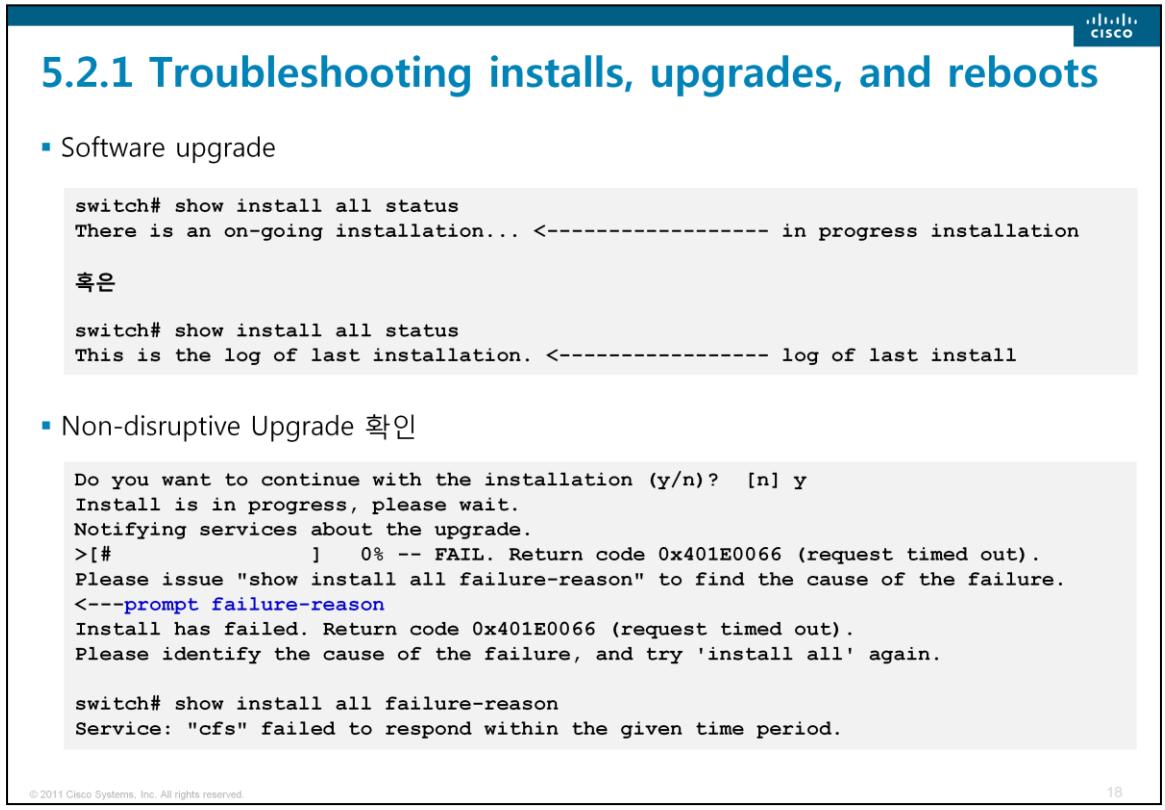
Tip 중에 하나는 log 파일을 확인 하는 것입니다.

버퍼에 저장된 log는 시스템이 리부팅하면 확인 할 수 없으나 nvram에 저장된 log는 재부팅 후에도 확인이 가능합니다.

Priority 0, 1, 2에 해당되는 system messages는 supervisor mdoule의 NVRMA에 저장됩니다.

따라서 스위치가 리부팅 된 후에도 show logging nvram 명령어를 사용하여 NVRAM에 저장된 syslog message를 확인 할 수 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



5.2.1 Troubleshooting installs, upgrades, and reboots

- Software upgrade

```
switch# show install all status
There is an on-going installation... <------------------ in progress installation

혹은

switch# show install all status
This is the log of last installation. <----------------- log of last install
```

- Non-disruptive Upgrade 확인

```
Do you want to continue with the installation (y/n)?  [n] y
Install is in progress, please wait.
Notifying services about the upgrade.
>[#                ]   0% -- FAIL. Return code 0x401E0066 (request timed out).
Please issue "show install all failure-reason" to find the cause of the failure.
<---prompt failure-reason
Install has failed. Return code 0x401E0066 (request timed out).
Please identify the cause of the failure, and try 'install all' again.

switch# show install all failure-reason
Service: "cfs" failed to respond within the given time period.
```

© 2011 Cisco Systems, Inc. All rights reserved.
18

NX-OS는 kickstart image 와 system image 두 개로 이미지로 이루어져 있습니다.
시스템을 구동 시키기 위해서는 두 개의 버전이 반드시 같아야 합니다.

업그레이드와 리부팅 작업은 운영, 유지 관리에 필요한 활동들로써 업그레이드 및 부팅 절차를 정확히 알고 있다면, 혹시라도 발생 할 수 있는 이슈를 원활히 해결 할 수 있게 됩니다.
show install all status 명령어를 이용하여 소프트웨어 업그레이드 진행 상황을 볼 수 있습니다.

또한 install all 명령어를 실행하게 되면 업그레이드가 진행되며 업그레이드를 할 수 있는 상태인지를 우선 체크하게 됩니다.

업그레이드 진행 중 어떤 이유에서든 failure가 발생한다면, 시스템은 리부팅이 되고 업그레이드는 실패하게 됩니다.

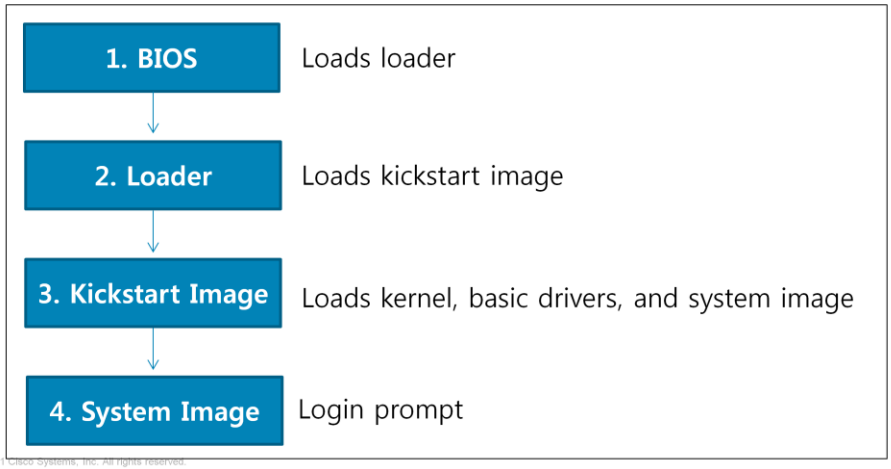
이런 이유를 알고 싶다면 show install all failure-reason 명령어를 이용하여 어떤 이유에 의해서 실패했는지를 볼 수 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

5.2.2 Troubleshooting installs, upgrades, and reboots

- 정상의 부팅은 아래와 같은 순서대로 진행

1. The basic input/output system (BIOS) loads the loader
2. The loader loads the kickstart image into RAM and starts the kickstart image
3. The kickstart image loads and starts the system image
4. The system image reads the startup-configuration file



© 2011 Cisco Systems, Inc. All rights reserved.

모든 device configuration은 internal bootflash에 위치합니다.
만약 internal bootflash에 문제가 생겼다면, configuration을 잃어 버릴 수도 있게 됩니다.
따라서 주기적인 저장과 backup이 필요하게 됩니다.

정상적인 시세템 부팅은 다음 순서대로 진행이 됩니다.

1)The basic input/output system (BIOS)이 loader를 load 합니다.
2)The loader는 kickstart image를 RAM으로 load하고 kickstart image를 구동합니다.
3)The kickstart image는 system image를 load하고 구동합니다.
4)The system image는 startup-configuration file을 읽습니다.

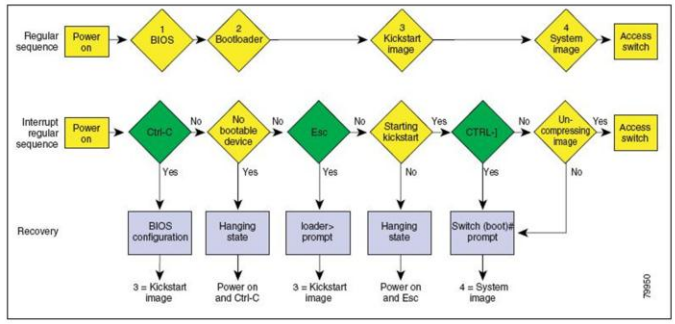
만약, system image가 파손되었다면, 진행이 되지 못하고 error state로 빠지게 될 것입니다.
이때 system boot sequence를 interrupt 시켜서 BIOS configuration utility로 들어가서 image를 recover 시킬 수 있습니다.

Caution: The internal sequence goes through four phases between the time that you turn on the system and the time that the system prompt appears on your terminal--BIOS, boot loader, kickstart, and system.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

5.2.3 Troubleshooting installs, upgrades, and reboots

- Regular and Recovery Sequence



- Recovery Interruption

단계	Normal Prompt	Recovery Prompt	설명
BIOS	loader>	No bootable device	BIOS가 self test, 메모리 test 시작, **Ctrl+C** 입력으로 BIOS 설정 모드 유틸리티 진입
Boot loader	Starting kickstart	loader>	Boot loader가 부팅하기 위하여 loaded 소프트웨어 uncompress 수행 **Esc** 입력으로 boot loader prompt 진입
Kickstart	Uncompressing system	switch(boot)#	Boot loader 단계 후 **Ctrl-]** 입력으로 switch(boot)# prompt 진입
System	Login:	--	System image가 configuration file을 load 함

© 2011 Cisco Systems, Inc. All rights reserved.
20

Supervisor module에서 loader> prompt 상태에서 recovery

Caution : 이 단계에서는 init system 명령어를 이용합니다. 이 명령어는 device의 file system을 reformat하게 됩니다. 이 명령어를 수행하기 전에 backup configuration이 있는지 확인하고 실행해야 합니다.

loader> 프롬프트는 정상적인 switch# 프롬프트와 완전히 다른 단계 입니다.

loader> 프롬프트 단계에서는 명령어 자동 완성 기능도 동작하지 않습니다. 따라서 정확히 모든 명령어를 타이핑 해야 합니다.

만약 이 loader> 프롬프트 단계에서 tftp를 이용해야 하는 상황이라면, 원격 서버의 이미지 위치를 full path로 타이핑 해야 합니다.

loader> Help 명령어를 이용하면 사용할 수 있는 명령어 리스트를 보여 줍니다.

Single supervisor module에서 kickstart image (system error state)가 문제가 생긴 경우 복구는 아래 단계로 진행하게 됩니다.

1. Enter the local IP address and subnet mask for the system at the loader> prompt, and press **Enter**.

loader> **set ip 172.16.1.2 255.255.255.0**

2. Specify the IP address of the default gateway.

loader> **set gw 172.16.1.1**

3. Boot the kickstart image file from the required server.

loader> **boot tftp://172.16.10.100/tftpboot/n7000-s1-kickstart-4.0.bin**

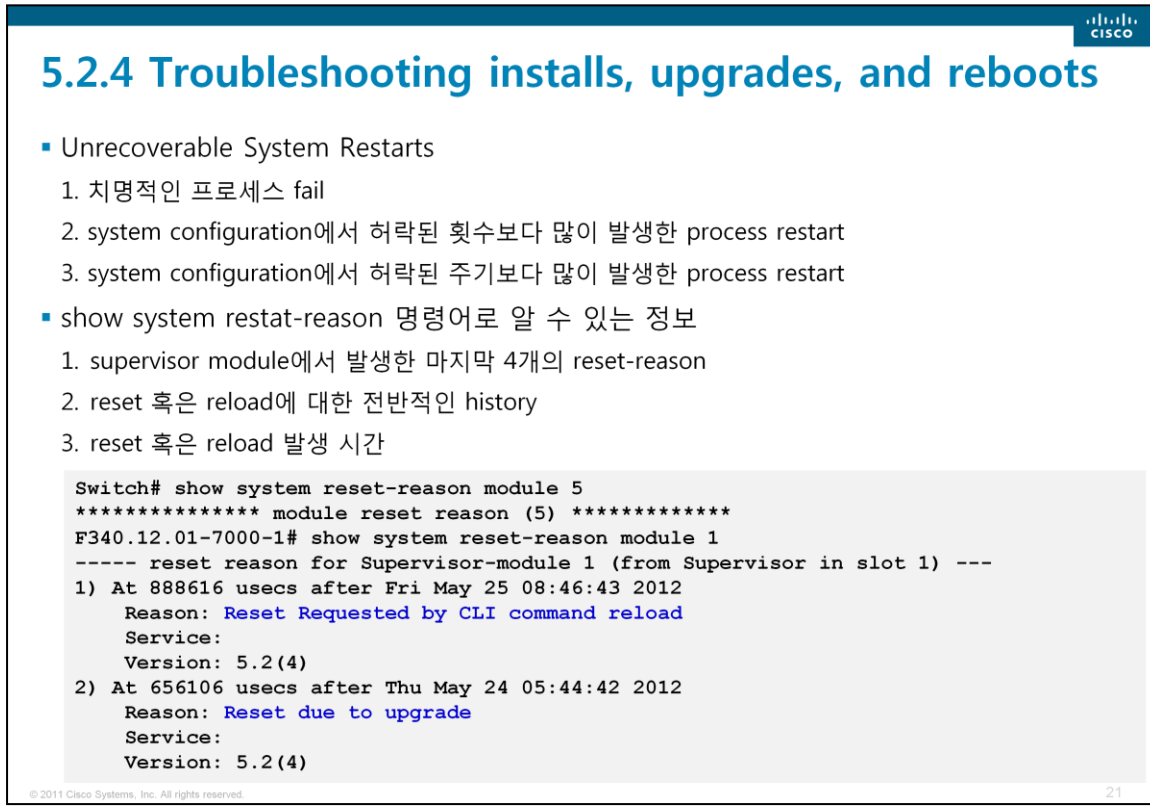
In this example, 172.16.10.100 is the IP address of the TFTP server, and n7000-s1-kickstart-4.0.bin is the name of the kickstart image file that exists on that server.

The switch(boot)# prompt indicates that you have a usable Kickstart image.

4. Enter the **init system** command at theswitch(boot)# prompt.

switch(boot)# **init system**

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



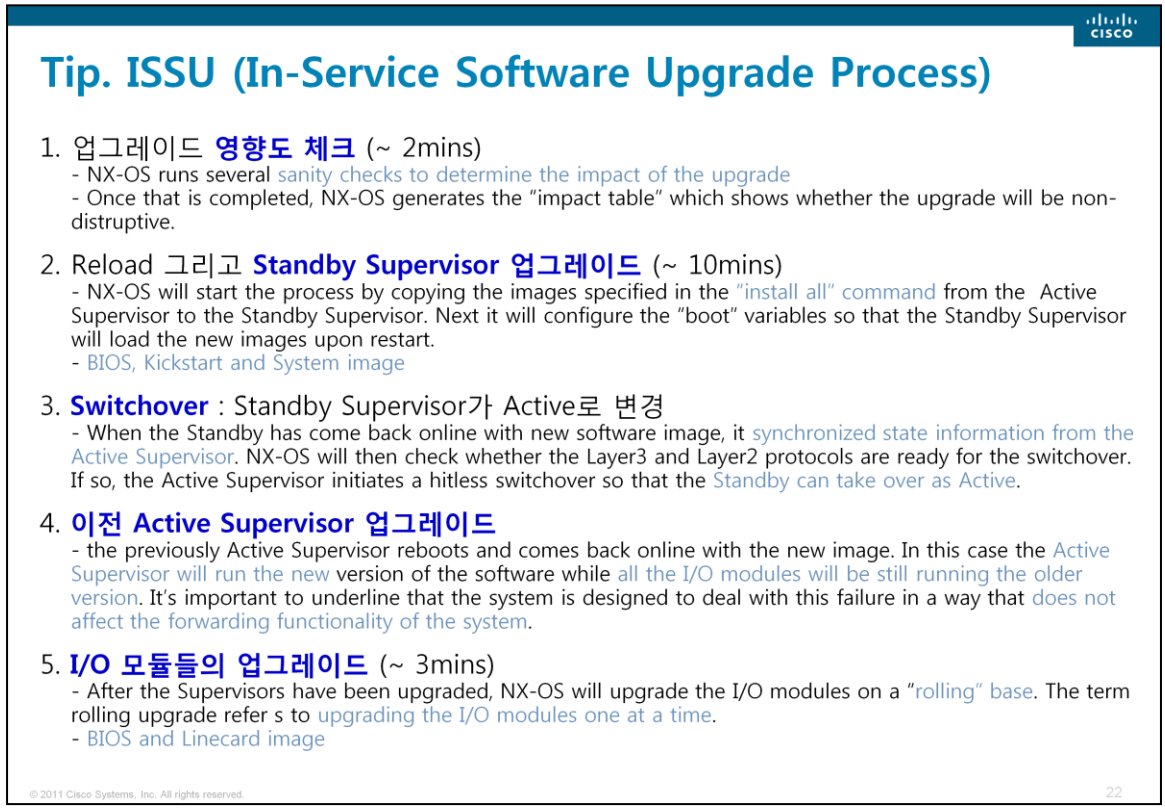
복구 할 수 없는 시스템 재기동은 다음과 같은 case에 발생하게 됩니다.

-치명적인 프로세스 에러 및 재구동이 불가능한 경우
-시스템에서 허락된 횟수 보다 많은 횟수 만큼 프로세스가 restart 된 경우
-시스템에서 허락된 횟수 보다 자주 프로세스 restart가 발생한 경우
-프로세스 reset 효과는 각 프로세스에 정의된 policy에 의해서 결정된다.
복구할 수 없는 reset은 특정 기능 정지, active supervisor restart, supervisor switchover, 혹은 시스템이 restart 될 수도 있다.

show system reset-reason 명령어를 이용하여 다음과 같은 정보를 획득할 수 있다.
최근 발생한 reset-reason을 4가지 저장하고 있다.
이 정보를 자세히 살펴 보면 최근 어떤 이유에 의해서 reset이 발생했는지 확인 할 수 있다.
또한 해당 모듈이 reset한 정확한 시간에 대한 정보도 획득할 수 있다.
더불어서 현재 운영 중이 OS 버전 정보도 같이 얻을 수 있다.

show module : serial number 등을 포함하여 'module'의 상태 표시
show system reset-reason : 각 supervisor engine의 reset reason 표시
show logging nvram : persistent store 에 저장된 severity level이 포함된 syslog 정보 표시
show system reset-reason module <x> : Displays the reset-reason of a given module if it is shutdown

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



ISSU (upgrade) 혹은 ISSD (downgrade)는 시스템이 운영 중 OS를 업그레이드 하거나 다운그레이드 하는 것을 말합니다. 시스템 운영 중에 행해지는 행위이므로 서비스 영향도가 없는 것이 특징이라 하겠습니다.

위에 슬라이드에서 보시는 것처럼 ISSU를 실행하게 되면 시스템 내부적으로 총 6단계에 걸쳐서 각각 진행이 된다고 보시면 됩니다. 또한 각 단계별로 소요되는 대략적인 시간도 표시가 되어 있으나 장착된 모듈의 수 등에 따라서 총 소요 시간은 다소 차이가 발생하게 됩니다.

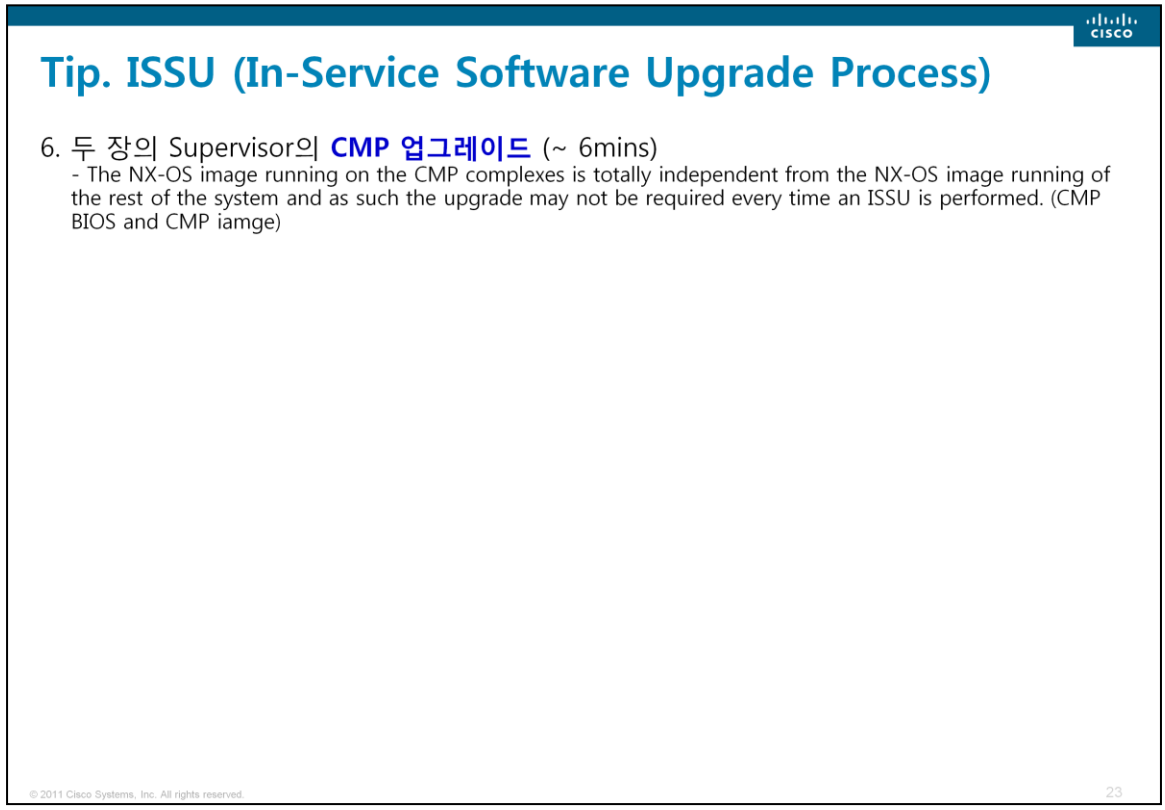
우선 ISSU를 실행하시게 되면, 업그레이드를 하기 전에 ISSU를 통해서 서비스 중 문제 없이 업그레이드가 가능한지에 대한 체크를 먼저 하게 됩니다. 혹시라도 각 체크 항목 중에서 이슈가 될 만한 부분이 있다면 ISSU는 종료가 됩니다. 해당 내용을 잘 체크하셔서 조금 있다가 다시 시도할지 아니면 해당 이슈를 제거하고 시도할지를 판단 할 수 있게 됩니다.

문제없이 업그레이드를 진행할 수 있다고 판단되면, standby supervisor engine을 우선 업그레이드 하게 됩니다. Standby supervisor engine이 새로운 OS를 가지고 정상적으로 부팅이 되면, swithchover해서 자신이 새로운 active engine 역할을 하게 됩니다.

따라서 이제 막 standby supervisor engine이 모듈을 대상으로 OS 업그레이드 작업을 진행하게 됩니다.
이때에는 잠시 동안 두 개의 다른 OS 버전으로 supervisor engine이 구동 되는 상태가 됩니다.

두 장의 supervisor engine이 모두 OS 업그레이드가 끝났다면, 이제 곧이어 각각의 I/O (라인카드)을 대상으로 업그레이드가 진행됩니다. 물론 각 라인카드 OS 업그레이드 중에도 서비스 영향은 없습니다. 그 자세한 이유는 다음 슬라이드를 참고해 주세요.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



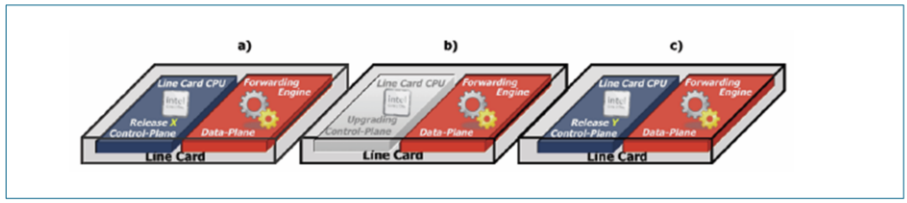
모든 I/O 모듈의 control plane 업그레이드를 마쳤다면,
이제 각 Supervisor engine안의 독립된 영역인 CMP 영역에 대한 업그레이드가 진행됩니다.

CMP는 간단히 말씀드려면 독립적인 management 콘솔이라고 보시면 됩니다. 별도의 CPU, RAM, Disk를 가지고 있어서 Nexus 스위치에 전원이 공급되는 한 supervisor engine의 control plane과 독립적으로 구동되면서 management 연결을 수용하게 됩니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

Tip. ISSU (Upgrade of the I/O modules)

1. Soon after the Active Supervisor notifies the I/O module about the upcoming upgrade, the software application (ex-netflow, FIB manger) running on the I/O module save their runtime data, which are then sent to the Active Supervisor where they will be stored the entire duration of the upgrade
2. NX-OS will then reboot the I/O module's control plane. While the control plane is being upgraded the data plane remains active so the ASIC-based forwarding engine can still forward traffic
3. As soon as the control plane of the I/O module is up and running with the new image, the Supervisor will restore the runtime data saved by the I/O module before the reboot



* The ability to clearly separate the data plane from the control plane is the key that allows the Nexus 7000 to provide a non-distruptive ISSU

© 2011 Cisco Systems, Inc. All rights reserved.
24

Supervisor engine, I/O 모듈, CMP OS가 모두 업그레이드를 마쳤습니다.

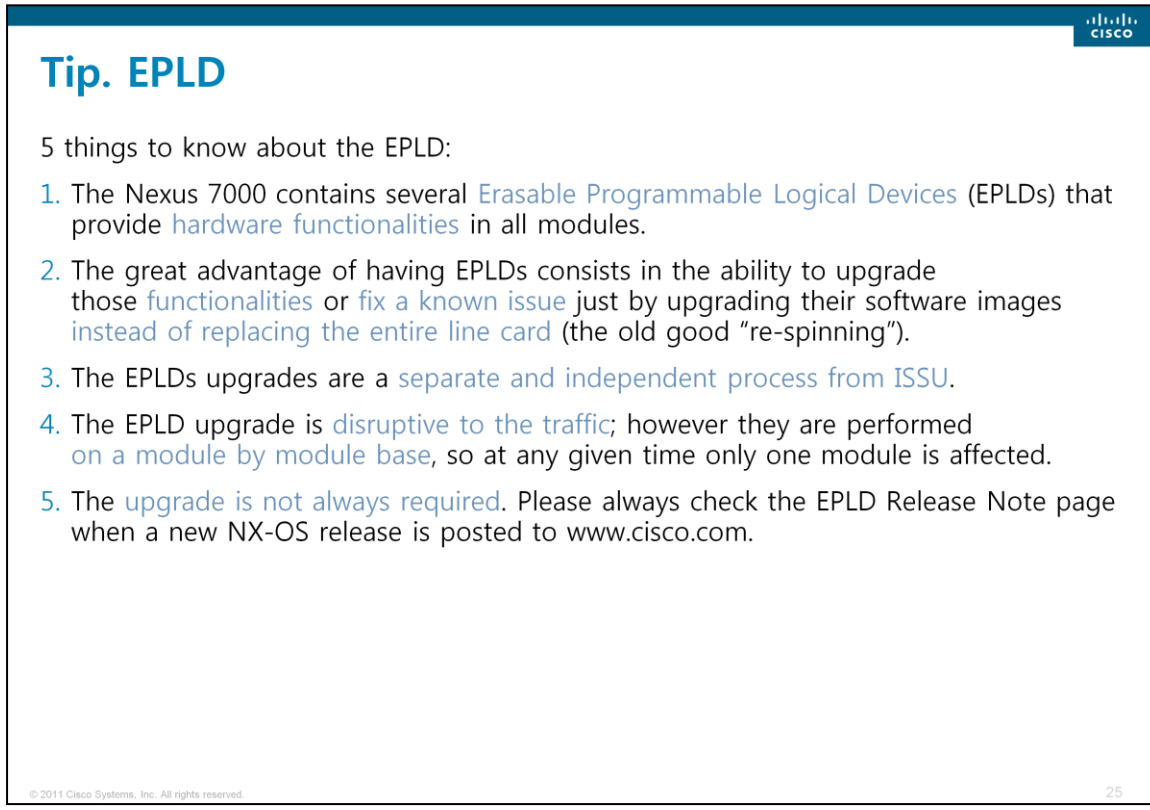
그럼 앞서 말씀드린대로 패킷 포워딩을 하는 중에 OS를 업그레이드 하더라도 서비스에 영향이 없는 이유를 간단히 살펴 보도록 하겠습니다.

Active supervisor engine은 업그레이드가 될 I/O 모듈쪽으로 업그레이드가 임박했음을 알게 됩니다.
이 메시지를 받은 I/O 모듈은 I/O 모듈에서 구동되는 소프트웨어 어플리케이션 (ex-netflow, FIB manager)의 정보를 저장하고 active supervisor로 보내서 업그레이드가 진행되는 동안 해당 정보가 supervisor에 저장 되도록 하게 됩니다.

그리고 해당 I/O 모듈의 control plane 부분의 업그레이드가 진행되게 됩니다.
이때 data plane은 여전히 active 상태로 패킷 포워딩을 하게 됩니다.

I/O 모듈의 control plane 업그레이가 완료되면 supervisor 에 저장된 정보가 I/O 모듈로 restore 됩니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



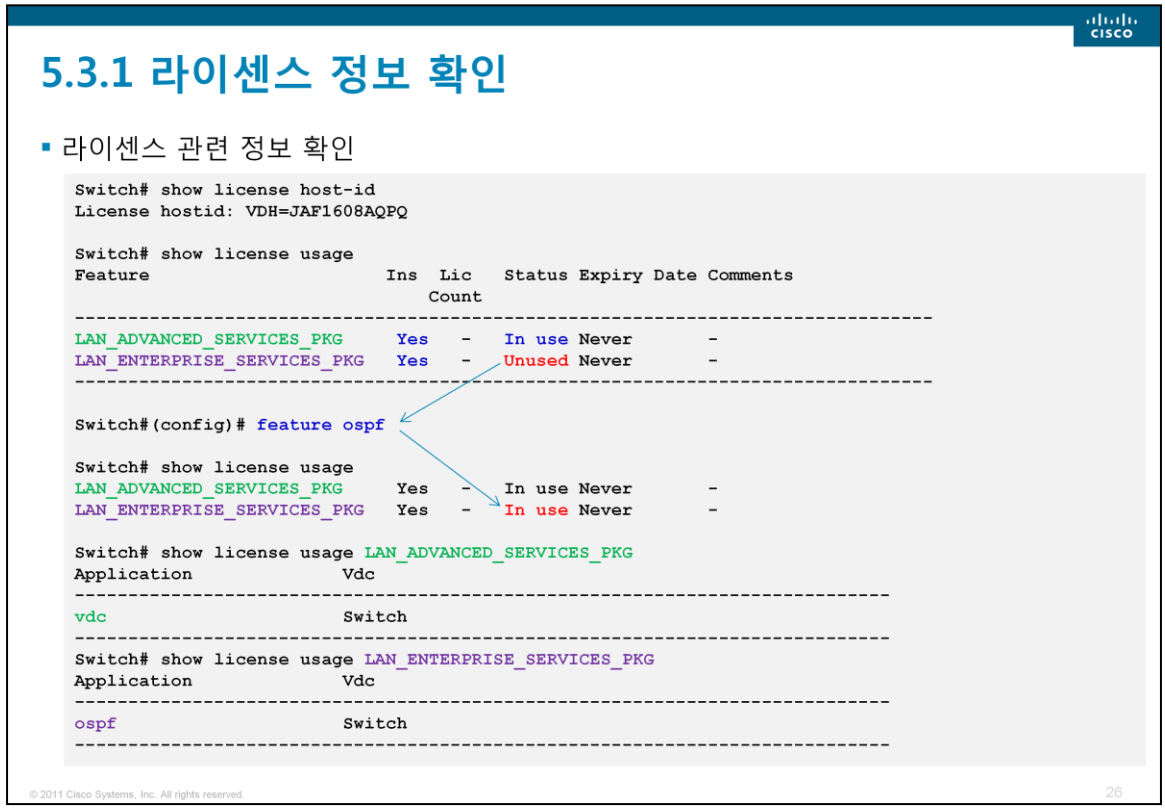
ISSU와는 별도로 EPLD가 진행되어야 하는 경우가 있습니다.

ISSU와 함께 반드시 EPLD 업그레이드가 진행되어야 하는 것은 아니지만 권고 사항이므로 같이 업그레이드 하시는 것이 좋습니다.

업그레이드 버전에 따라서 혹은 사용하려는 new feature에 따라서 EPLD 업그레이드가 반드시 필요한 부분도 있게 됩니다.

중요한 것은 EPLD 업그레이드에는 서비스 영향도가 발생하므로 EPLD를 ISSU와 동시에 진행해야 한다면 서비스 영향 최소화를 위해서 계획휴지를 잡으시고 작업하셔야 합니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



NX-OS는 사용하는 feature, 하드웨어 성능, 기능에 따라서 별도의 라이센스를 필요로 하게 됩니다.

대부분은 시스템 기반으로 설치가 되지만 어떤 경우는 각 라인카드 별로 라이센스가 필요하게 되는 경우도 있습니다.

라이센스 설치를 하지 않고 feature를 enable해서 일정 기간 사용할 수 있는데 이런 기간을 'grace period'라고 합니다.

Chassis Serial Numbers

라이센스는 인스톨이 되어야 하는 샤시의 serial number를 이용해서 발급을 받게 됩니다. 샤시 시리얼 번호로 받은 라이센스 파일은 다른 시스템에 사용하실 수가 없습니다.

Swapping out a Chassis

만약 샤시 불량 등으로 샤시를 교체하셨다면, cisco 라이센싱팀을 contact 하시거나 TAC을 contact 하셔서 해당 샤시에 필요한 새로운 라이센스 파일을 발급받아서 설치 하셔야 합니다. 과거 라이센스 파일은 새로운 샤시에는 사용하실 수 없습니다.

Grace Period

만약 어떤 feature가 특별한 라이센스가 필요한데, 라이선스를 구매하지 않으셨다면, 120 day grace period 동안 해당 feature를 사용하실 수 있습니다. 그러나 해당 평가판 기간이 종료가 되면 해당 feature는 사용할 수 없게 되므로 반드시 라이선스를 구매해서 인스톨을 하셔야 합니다.

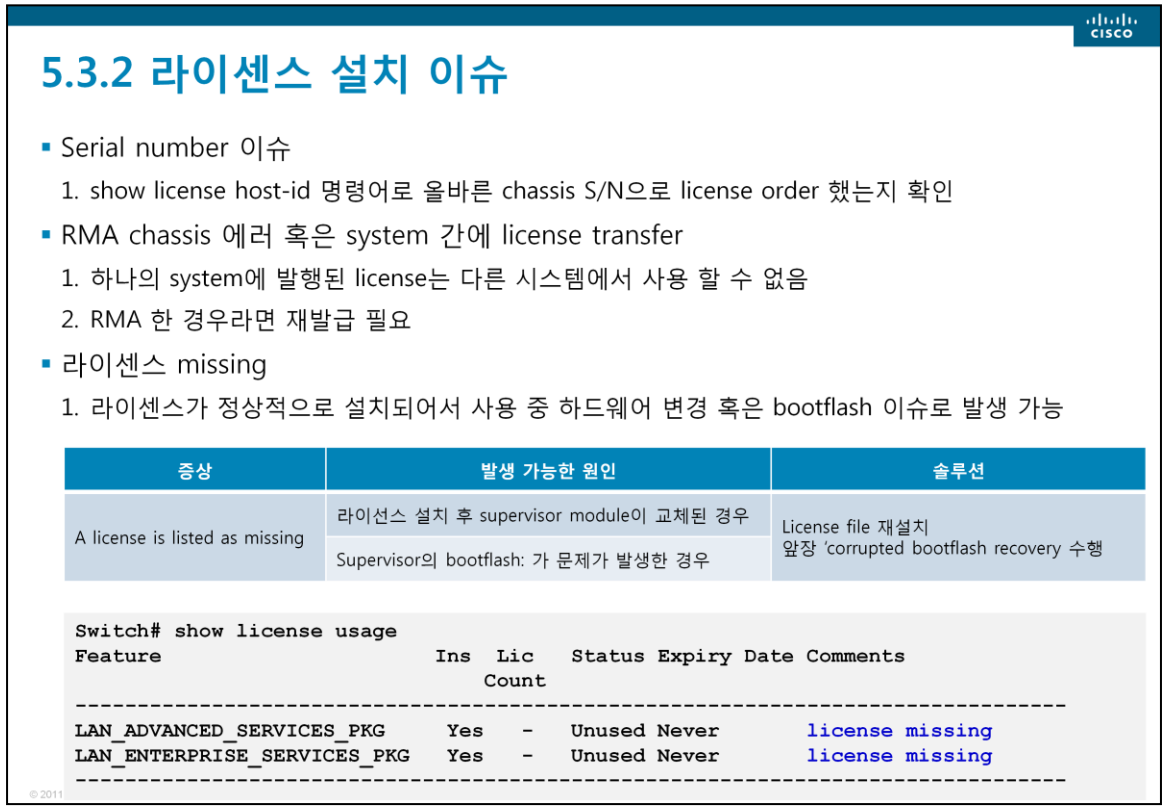
라이센스 패키지는 여러 가지로 구분이 되므로 show license usage를 통해서 확인 하실 수 있습니다.

위에 보시는 것처럼 라이선스를 발급 받기 위해서는 show license host-id 명령어를 통해서 해당 샤시의 serial number를 확인하시고 신청하셔야 합니다.

또한 show license usage 명령어를 이용하시면 현재 어떤 종류의 라이선스가 설치 되어 있고, 현재 해당 라이선스와 연관된 feature가 enable 되어 있는지 여부를 확인 하실 수 있습니다. 라이선스는 install했지만 관련된 feature를 사용하지 않는다면 'Unused'로 표시가 되며, 관련된 feature를 enable 한 후에 다시 보게되면 'In use'라고 바뀌는 것을 보실 수 있습니다.

또한 show license usage 뒤에 각 라이선스 타입을 치시면 해당 라이선스에 해당되는 feature가 보여지게 됩니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



TAC에서 Case 처리를 하다보면 라이센스와 관련된 case가 간혹 열리는데, 라이선스 파일의 발급이 잘 못 된 경우가 종종 있게 있습니다.

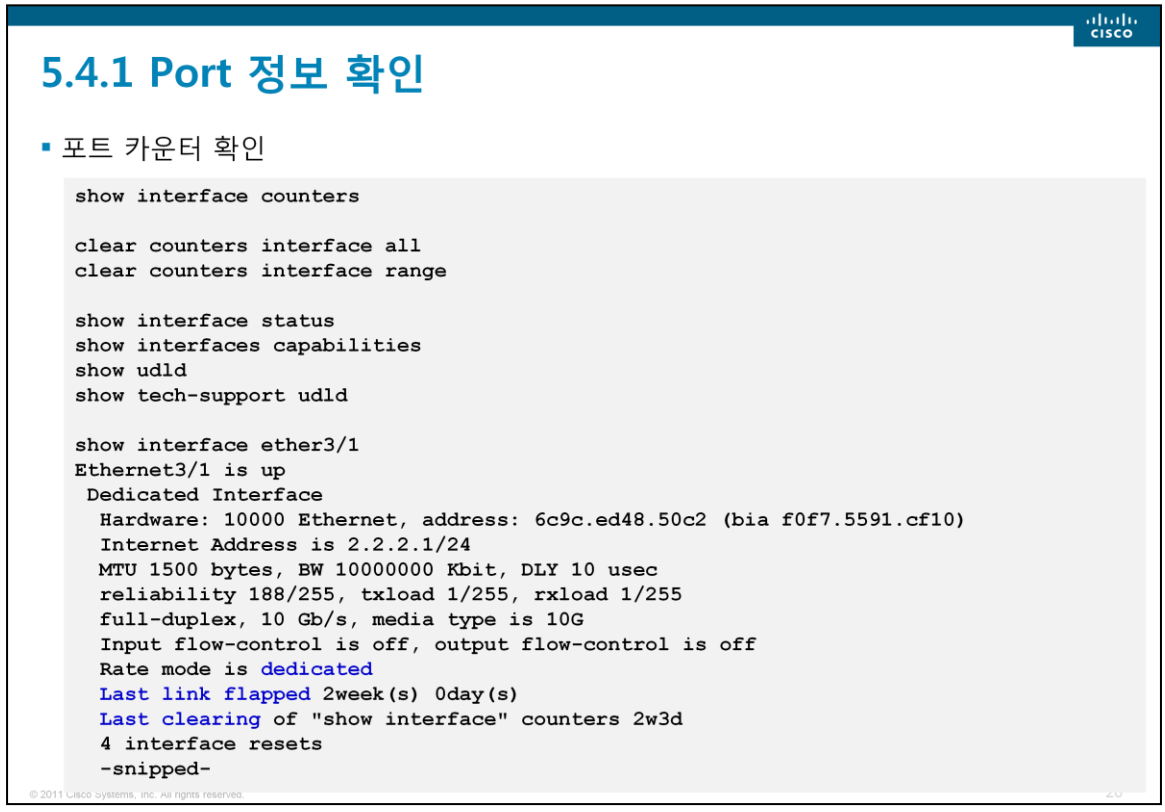
제품 구매 시 라이센스를 정확히 구매하셨고, 올바른 샤시 시리얼 번호로 발급을 받았고, 해당 샤시에 인스톨이 잘 되었고 activation이 되었는지를 먼저 확인 하시면 좋을 것 같습니다.

혹시 여러 대의 샤시에 대한 라이센스를 받으시는 경우 종종 다른 샤시에 라이선스 파일을 인스톨하면서 발생하는 경우도 있습니다.

라이센스와 연관된 문제가 생긴다면 적어도 아래 명령어를 통해서 자료를 수집하시고 TAC으로 케이스를 열어 주시면 됩니다.

show log
show license
show license brief
show license usages
show license usages [각 라이선스 패키지]
show license host-id.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



Port Guidelines

포트 인터페이스 설정 전 show module을 통하여 해당 모듈이 정상적으로 작동하는지 확인을 합니다.

특히 일부 모듈에서 활용하는 dedicate mode 혹은 shared mode 기능이 되어 있는지 확인을 해야 합니다.

Dedicated mode에서는 4개가 하나의 그룹으로 묶인다면 한 포트만 사용가능하고 나머지 3포트는 사용할 수 없게 됩니다.

인터페이스에서 확인 할 수 있는 항목에 대한 설명은 아래 내용을 참고해 주세요

FCS-Err is the number of valid size frames with FCS (Frame Check Sequence) errors but no framing errors: this is typically a physical issue (cabling, bad port, NIC card,) but can also indicate a duplex mismatch

Align-Err is the number of frames with alignment errors (frames that do not end with an even number of octets and have a bad CRC) received on the port; these usually indicate a physical problem (cabling, bad port, NIC card,? but can also indicate a duplex mismatch; when the cable is first connected to the port, some of these errors may occur; also, if there is a hub connected to the port then collisions between other devices on the hub may cause these errors

Runts are frames received that are smaller than the minimum IEEE 802.3 frame size (64 bytes for Ethernet) and with a bad CRC; this can be caused by duplex mismatch and physical problems like a bad cable, port, or NIC card on the attached device

Late-Coll (Late Collisions) is the number of times that a collision is detected on a particular port late in the transmission process; for a 10mbit/s port this is later than 512 bit-times into the transmission of a packet; five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system; this error can indicate a duplex mismatch among other things; for the duplex mismatch scenario the late collision would be seen on the half duplex side; as the half duplex side is transmitting, the full duplex side does not wait its turn and transmits simultaneously causing a late collision; late collisions can also indicate an Ethernet cable/segment that is too long; collisions should not be seen on ports configured as full duplex

Single-Coll (Single Collision) is the number of times one collision occurred before the port transmitted a frame to the media successfully; collisions are normal for port configured as half duplex but should not be seen on full duplex ports; if collisions are increasing dramatically this points to a highly utilized link or possibly a duplex mismatch with the attached device

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

5.4.1 Port 정보 확인

- 포트 카운터 확인

```
show interface counters

clear counters interface all
clear counters interface range

show interface status
show interfaces capabilities
show udld
show tech-support udld

show interface ether3/1
Ethernet3/1 is up
 Dedicated Interface
  Hardware: 10000 Ethernet, address: 6c9c.ed48.50c2 (bia f0f7.5591.cf10)
  Internet Address is 2.2.2.1/24
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec
  reliability 188/255, txload 1/255, rxload 1/255
  full-duplex, 10 Gb/s, media type is 10G
  Input flow-control is off, output flow-control is off
  Rate mode is dedicated
  Last link flapped 2week(s) 0day(s)
  Last clearing of "show interface" counters 2w3d
  4 interface resets
  -snipped-
```

© 2011 Cisco Systems, Inc. All rights reserved.

Multi-Coll (Multiple Collision) is the number of times multiple collisions occurred before the port transmitted a frame to the media successfully; collisions are normal for port configured as half duplex but should not be seen on full duplex ports; if collisions are increasing dramatically this points to a highly utilized link or possibly a duplex mismatch with the attached device

Excess-Coll (Excessive Collisions) is a count of frames for which transmission on a particular port fails due to excessive collisions; an excessive collision happens when a packet has a collision 16 times in a row; the packet is then dropped; excessive collisions is typically an indication that the load on the segment needs to be split across multiple segments but can also point to a duplex mismatch with the attached device; collisions should not be seen on ports configured as full duplex

Undersize are frames received that are smaller than the minimum IEEE 802.3 frame size of 64bytes long (excluding framing bits, but including FCS octets) that were otherwise well formed; check the device sending out these frames

Giants exceed the maximum IEEE 802.3 frame size (1518 bytes for non-jumbo Ethernet); try to find the offending device and remove it from the network?

Carri-Sen (Carrier Sense) occurs every time an Ethernet controller wants to send data on a half duplex connection; the controller senses the wire and check if it is not busy before transmitting; this is normal on an half-duplex Ethernet segment

www.cisco.com/warp/public/473/164.html#show_interface

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

5.4.2 ErrorDisable

- 스위치가 감지해서 해당 포트를 disabled로 만들 포트 확인

```
switch# show interface e1/14
e1/7 is down (errDisabled)
```

- Cable, SFP, Optic 확인
- 해당 포트의 internal state transition 확인 (capability mismatch)

```
switch# show system internal ethpm event-history interface e1/7
>>>>FSM: <e1/7> has 86 logged transitions<<<<<
1) FSM:<e1/7> Transition at 647054 usecs after Tue Jan  4 06:54..
    Previous state: [ETH_PORT_FSM_ST_NOT_INIT]
    Triggered event: [ETH_PORT_FSM_EV_MODULE_INIT_DONE]
    Next state: [ETH_PORT_FSM_ST_IF_INIT_EVAL]
2) FSM:<e1/7> Transition at 647114 usecs after Tue Jan  4 06:54..
    Previous state: [ETH_PORT_FSM_ST_INIT_EVAL]
    Triggered event: [ETH_PORT_FSM_EV_IE_ERR_DISABLED_CAP_MISMATCH]
    Next state: [ETH_PORT_FSM_ST_IF_DOWN_STATE]
```

- 스위치 로그 확인

```
switch# show logging logfile
Jan  4 06:54:04 switch %PORT_CHANNEL-5-CREATED: port-channel 7 created
Jan  4 06:54:24 switch %PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel 7 is down
(No operational members)
Jan  4 06:54:40 switch %PORT_CHANNEL-5-PORT_ADDED: e1/8 added to port-channel 7
Jan  4 06:54:56 switch %PORT-5-IF_DOWN_ADMIN_DOWN: Interface e1/7 is down (Admnistratively down)
Jan  4 06:54:59 switch %PORT_CHANNEL-3-COMPAT_CHECK_FAILURE: speed is not compatible
Jan  4 06:55:56 switch%PORT_CHANNEL-5-PORT_ADDED: e1/7 added to port-channel 7
```

© 2011 Cisco Systems, Inc. All rights reserved.

NX-OS는 인터페이스가 down이 된 경우 자세한 내용, 즉 그 이유에 대해서도 알려 줍니다.

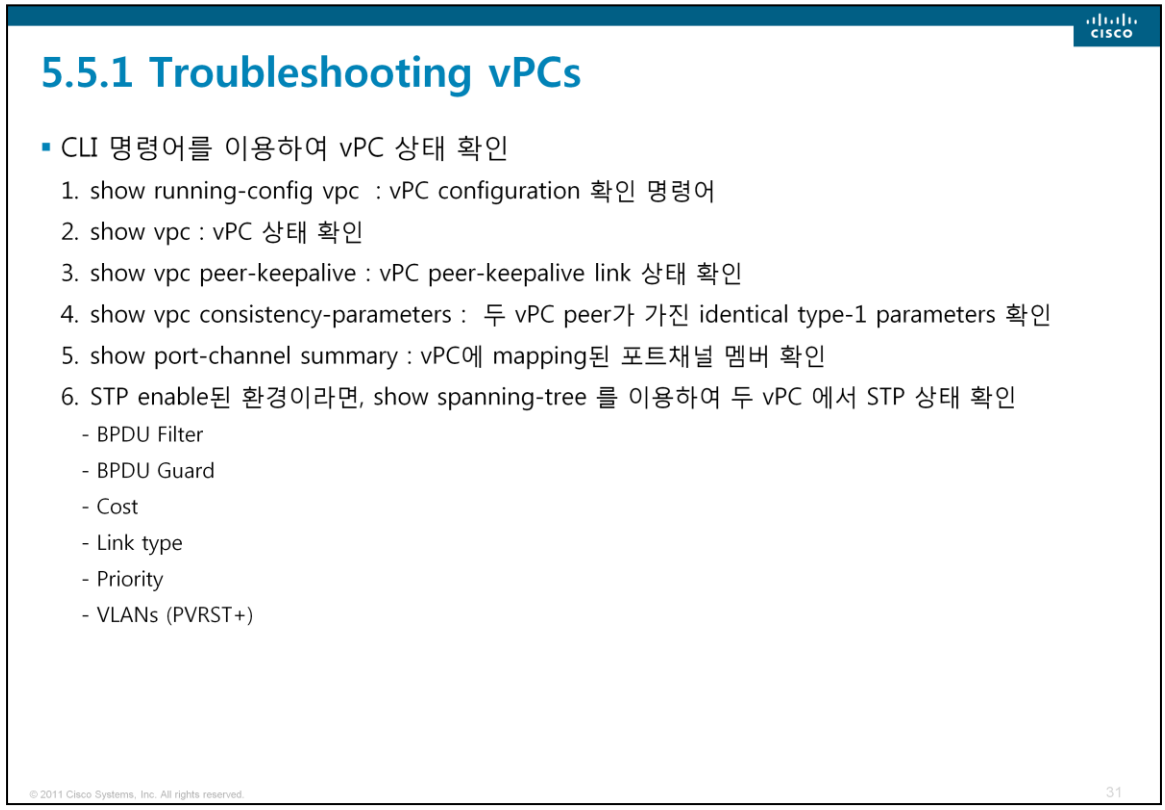
포트 레벨에서 문제가 생겼다면 스위치 로그와 함께 해당 모듈의 포트 레벨에서 발생하는 로그를 같이 보면 조금 더 구체적으로 볼 수 있습니다.

위의 예처럼,
특정 시간대 발생한 아래 로깅과 함께 특정 포트에 발생한 system 레벨의 로깅을 함께 비교해서 보시면 됩니다.

Jan 4 06:54:59 switch %PORT_CHANNEL-3-COMPAT_CHECK_FAILURE: speed is not compatible

2) FSM:<e1/7> Transition at 647114 usecs after Tue Jan 4 06:54..
Previous state: [ETH_PORT_FSM_ST_INIT_EVAL]
Triggered event: [ETH_PORT_FSM_EV_IE_ERR_DISABLED_CAP_MISMATCH]
Next state: [ETH_PORT_FSM_ST_IF_DOWN_STATE]

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



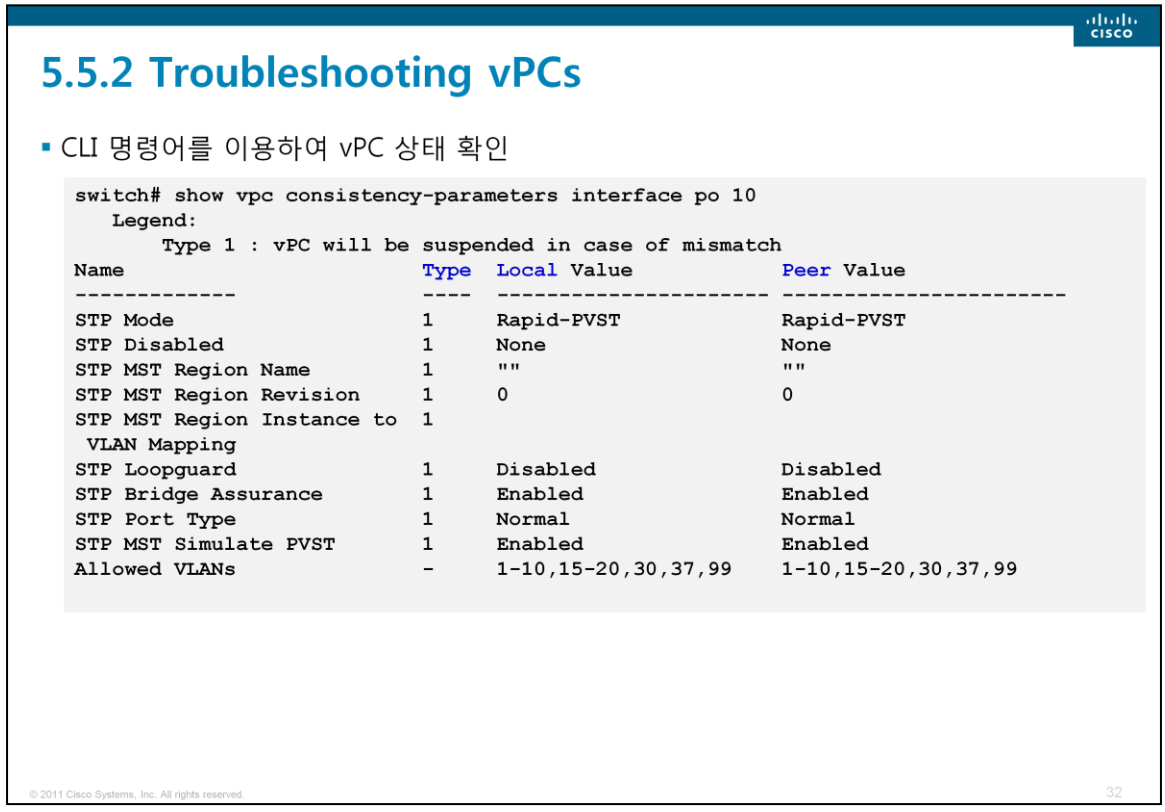
이번 장은 vPC 트러블슈팅에 대해서 간단히 살펴 보겠습니다.

vPC 구성 상태에서 이슈가 생긴 경우라면 최소한 아래와 같은 명령어를 통해서 자료를 수집해야 합니다.

show running-config vpc
show vpc
show vpc peer-keepalive
show vpc consistency-parameters
show port-channel summary
STP enable된 환경이라면, show spanning-tree 를 이용하여 두 vPC 에서 STP 상태 확인

각각의 명령어를 이용하여 configuration, vPC 간의 상태 확인, vPC keepalive 상태, 그리고 두 vPC device간 consistency parameter 가 모두 일치하는지 확인이 필요합니다. 또한 vPC에 매핑된 포트채널도 학인하시고 STP가 enable된 환경이라면 STP 관점에서의 L2 구성의 확인이 필요하게 됩니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



5.5.2 Troubleshooting vPCs

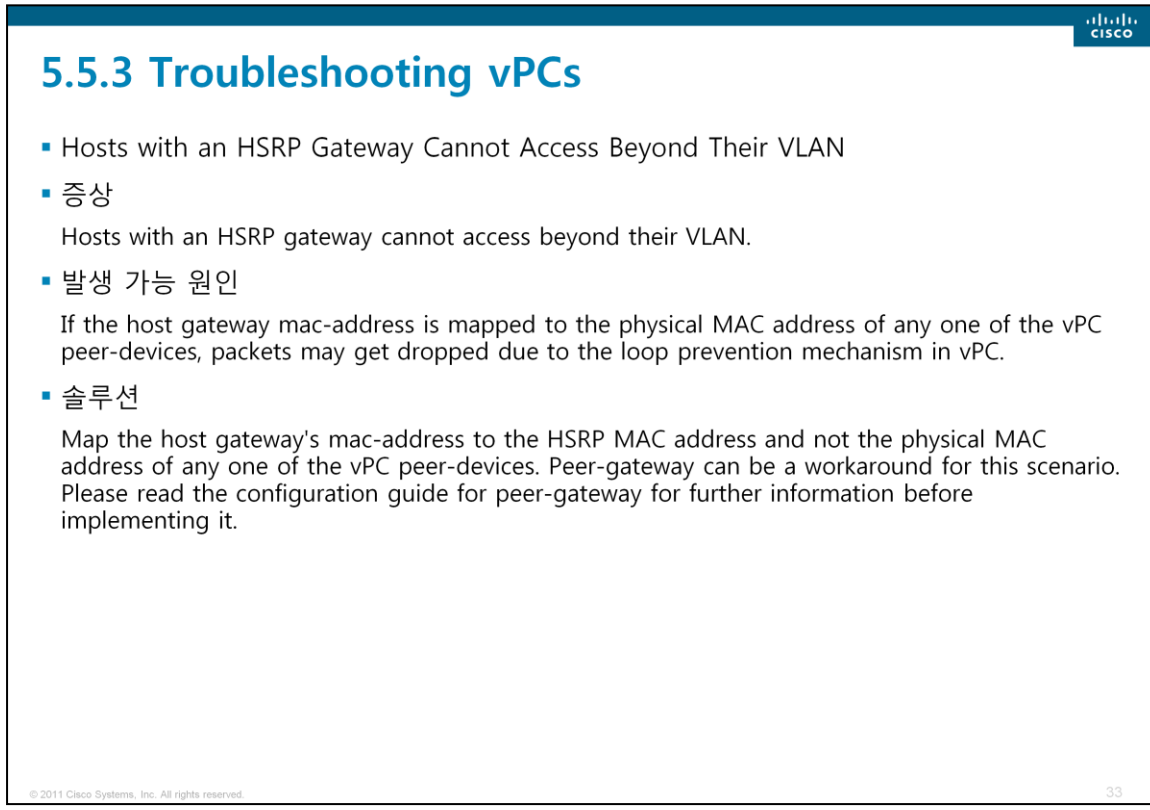
- CLI 명령어를 이용하여 vPC 상태 확인

```
switch# show vpc consistency-parameters interface po 10
   Legend:
       Type 1 : vPC will be suspended in case of mismatch
Name                        Type  Local Value            Peer Value
-------------               ----  ---------------------- -----------------------
STP Mode                    1     Rapid-PVST             Rapid-PVST
STP Disabled                1     None                   None
STP MST Region Name         1     ""                     ""
STP MST Region Revision     1     0                      0
STP MST Region Instance to  1
 VLAN Mapping
STP Loopguard               1     Disabled               Disabled
STP Bridge Assurance        1     Enabled                Enabled
STP Port Type               1     Normal                 Normal
STP MST Simulate PVST       1     Enabled                Enabled
Allowed VLANs               -     1-10,15-20,30,37,99    1-10,15-20,30,37,99
```

© 2011 Cisco Systems, Inc. All rights reserved.

위에 명령어를 이용하여 두 Peer간 (local , peer) 값을 확인 하실 수 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



간혹 열리는 case 중에는 vPC구성에서 Standby HSRP로 ping이 안되는 이슈에 대해서 무의 하는 경우가 있습니다.

vPC에 연결되는 end device에 따라서 다르지만 스토리지 혹은 L4와 같이 고성능이 요구되어 지는 장비의 경우 표준을 생략하고 성능에 초점을 맞춤으로써 이슈가 발생하는 경우가 있습니다. 자세한 설명은 아래 내용을 참고해 주세요.

기본적으로 표준에 의해서 잘 구현된 장비인 경우 특별히 vPC peer-gateway 명령어는 필요게 됩니다.

그러나 아래 CCO의 예처럼 성능을 위해서 일부 장비(NAS, L4)들의 동작 방식이 일반적이 않은 경우가 있습니다. 즉, 해당 장비에서는 N/W 장비의 HSRP VIP가 있음에도 불구하고 바로 물리적인 mac으로 트래픽을 전달하는 경우가 그 이유 입니다. 이런 경우 '문제가 발생'하기 보다는 '비효율적인 구조'가 되기도 하고 상단의 경로에 대한 라우팅이 두 장비가 다를 경우에는 통신이 안되기도 합니다. 즉, vPC (포트채널)를 통해서 primary 혹은 secondary vPC device로 갈 수 있는 경로가 있는 경우, primary vPC device가 패킷이 secondary vPC mac을 destination으로 하는 frame이 들어왔다면, primary vPC device는 vPC link를 통해서 secondary vPC device로 보내야 하는 비효율적인 트래픽 플로우가 발생 할 수 있습니다.

또한, 아래 vPC peer-gateway 명령어를 사용해야 하는 이유로 'built in vPC loop avoidanace mechanism'이라고 설명은 나와 있으나, 엄밀히 말하면, 'duplicate avoidance' 이라는 표현이 더 적합합니다. 즉, loop이 아니라 패킷 중복이 발생 할 수 있는 가능성 있다는 의미 입니다.

peer-gateway를 사용하는 목적은 위에서처럼 단말이 어떤 이유에 의해서 HSRP VIP가 아닌 BIA로 직접 패킷을 만들어서 보내는 경우, 자신이 가지고 있는 mac이 아닌 frame에 대해서 vpc-link를 통해서 옆으로 보내는 것이 아니라 자신이 'active router'로 동작하게 하는 것이다.

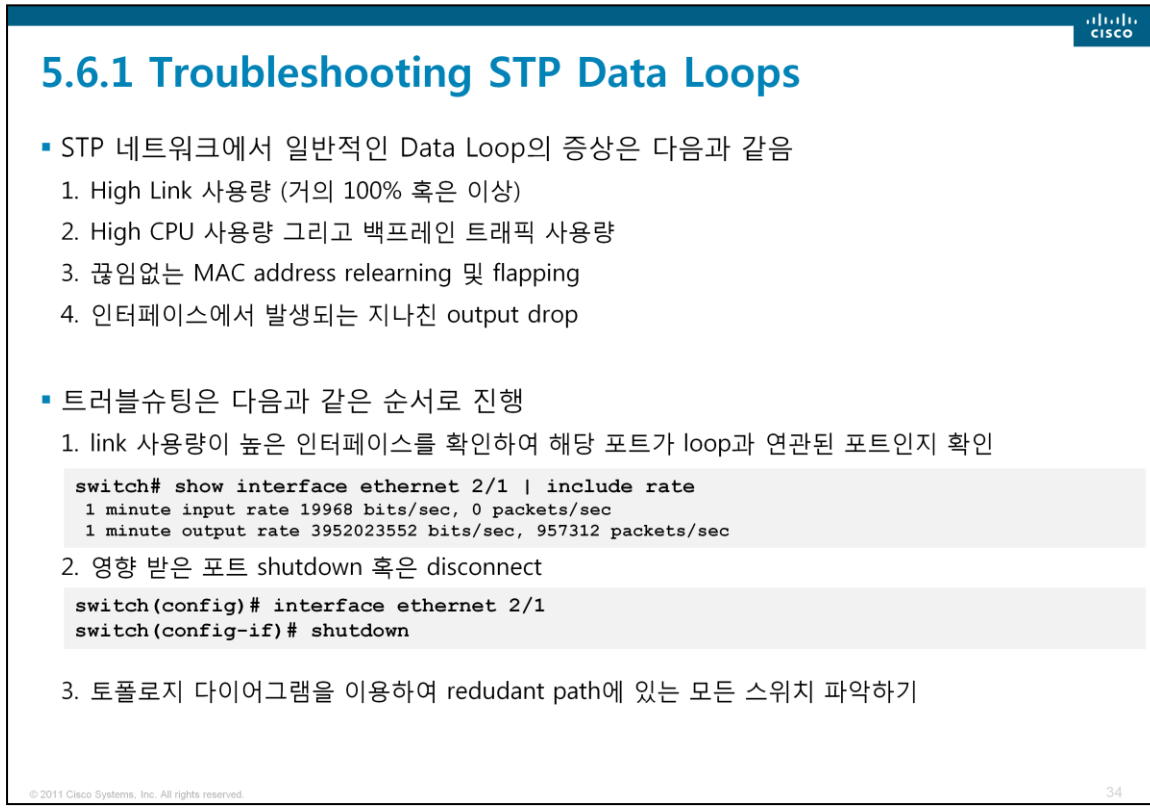
Packets reaching a vPC device for the non-local router MAC address are sent across the peer-link and could be dropped by the built in vPC loop avoidance mechanism if the final destination is behind another vPC.

When HSRP is enabled on both vPC peer devices on a VLAN and hosts on that VLAN set the HSRP as their gateway, they may not able to reach anything outside their own VLAN.

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/interfaces/configuration/guide/if_vPC.html#wp1558675

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/interfaces/configuration/guide/if_vPC.html#wp1560238

All contents are Copyright © 2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



L2 STP 관련한 이슈가 발생한 경우라면 설정 및 동작 상태를 보기 위해서 아래와 같은 내용을 확인해야 합니다 .

show running-config spanning-tree
show spanning-tree summary
show spanning-tree detail
show spanning-tree bridge
show spanning-tree mst
show spanning-tree mst configuration
show spanning-tree interface *interface-type slot/port* [detail]
show tech-support stp
show spanning-tree vlan

위의 명령어들은 동일한 명령어를 여러 번 실행하여 문제가 발생 했을때 어떤 값, 카운터 들이 올라가는 확인 하는 것이 필수적입니다.

또한 STP 에 Loop 같은 이슈가 발생할 때에는 추가적으로 High CPU utilization, 특정 인터페이스의 load 증가, 인터페이스 drop, mac flap과 같은 로그 메시지, 주변 장비의 로그 및 영향 등 모두 한꺼번에 발생할 수 있고, 몇 가지만 동시에 발생할 수 있기 때문에 주의 깊에 장치를 지켜봐야 합니다.

짧은 시간에 많은 변화가 생기는 만큼 여러 번 명령어를 실행하여 자료를 수집하고, 아래와 같은 추가적인 명령어도 도움이 됩니다.

show spanning-tree blockedports : STP에 의해서 block이 되어진 포트 확인
show mac address-table dynamic vlan : 각 node에서 learning 혹은 aging 확인

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/layer2/configuration/guide/l2_nx-os_book.html

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

5.6.2 Troubleshooting STP Data Loops

- 트러블슈팅은 다음과 같은 순서로 진행

1. 영향을 받지 않은 스위치와 같이 동일한 STP root bride로 표시되는지 확인

```
switch# show spanning-tree vlan 9
VLAN0009
 Spanning tree enabled protocol rstp
  Root ID    Priority    32777''
             Address     0018.bad7.db15''
             Cost        4
```

2. lowest 포트를 이용하여 root bridge로 올바르게 보이는지 확인

```
switch# show spanning-tree vlan 9
VLAN0009
Spanning tree enabled protocol rstp
Root ID     Priority    32777
            Address     0018.bad7.db15
            Cost        4
            Port 385 (Ethernet3/1)
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

© 2011 Cisco Systems, Inc. All rights reserved.
35

앞 슬라이드에서 설명 드린 내용을 명령어를 이용하여 범위를 좁혀나가고 확인하는 방법에 대한 예입니다.
이렇게 이슈를 좁혀 가려면 기본적으로 L2에 대한 물리적인 연결, 논리적인 구성도 및 일반적인 L2의 모습을 알고 있는 것이 중요합니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

5.6.3 Troubleshooting STP Data Loops

- 트러블슈팅은 다음과 같은 순서로 진행

1. root port 및 alternate port가 규칙적으로 BPUD 수신하는지 확인

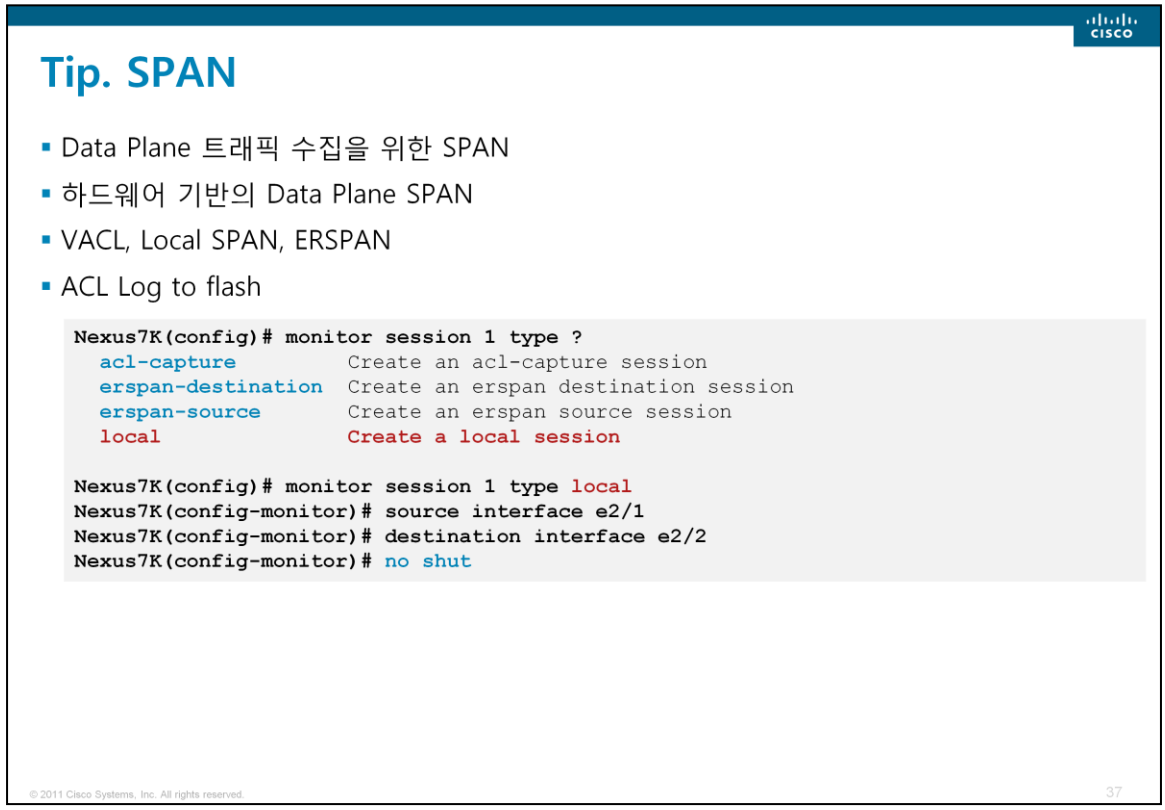
```
switch# show spanning-tree interface ethernet 3/1 detail
Port 385 (Ethernet3/1) of VLAN0001 is root forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.385
   Designated root has priority 32769, address 0018.bad7.db15
   Designated bridge has priority 32769, address 0018.bad7.db15
   Designated port id is 128.385, designated path cost 0
   Timers: message age 16, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port type is network by default
   Link type is point-to-point by default
   BPDU: sent 1265,  received 1269
```

2. BPDU를 정상적으로 수신하지 못한다면 다음 항목 확인 (하드웨어 패킷 통계 카운터)

```
--------------------------------------------------------------------------------
Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards
--------------------------------------------------------------------------------
mgmt0  --        --        --        --       --        --
Eth1/1  0         0         0         0        0         0
Eth1/2  0         0         0         0        0         0
Eth1/3  0         0         0         0        0         0
Eth1/4  0         0         0         0        0         0
Eth1/5  0         0         0         0        0         0
```

© 2011 Cisco Systems, Inc. All rights reserved.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



High CPU Utilization 현상은 다른 문제로 인해서 파생되어지는 경우가 많습니다.
따라서 High CPU 현상을 분석하기 위해서는 CPU로 보내지는 패킷을 수집해서 분석하는 것이 가장 효과적입니다.

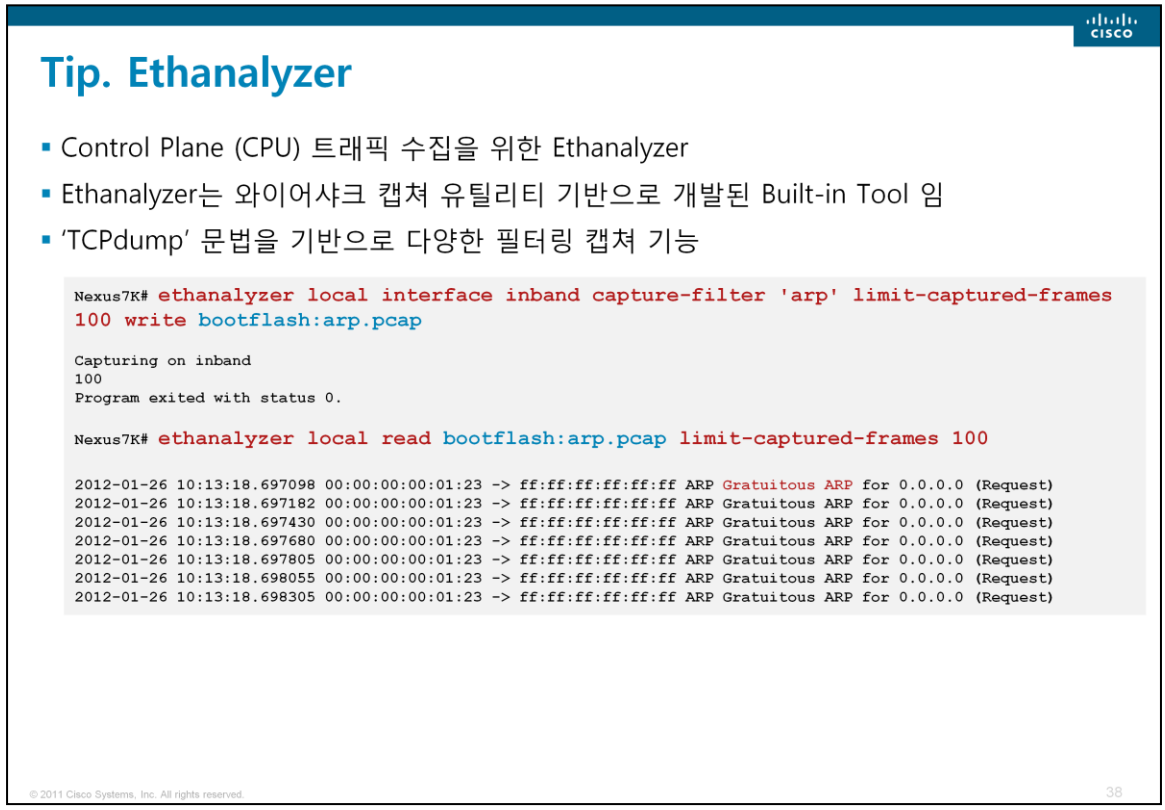
패킷을 분석하기 위해서는 일반적으로 '와이어샤크'와 같은 패킷 수집 어플리케이션을 이용하게 되는데, 별도의 PC에 설치해서 스위치에 연결하고 SPAN 기능을 이용해서 패킷을 수집해야 하는 단점이 있습니다.

NX-OS에서 Build-in 되어서 제공하는 Ethanalyzer (Ethernet Analyzer)를 활용하시면 CPU로 가는 inband 돌아다니는 패킷을 수집할 수 있습니다.

N7K-C# ethanalyzer local interface ?
bi-band Inband/Outband interface
mgmt Management interface

Inband라 함을 일반적으로 I/O 모듈에서 SUP로 올라가거나, CUP에서 I/O로 보내지는 길을 의미합니다.
즉, CPU 연결 인터페이스로 보시면 됩니다
Mgmt라 함은 mgmt0 인터페이스와 연관된 트래픽을 의미합니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



Ethanalyzer는 인터페이스-인터페이스 패킷은 수집할 수 없고, CPU의 Inband 만을 수집할 수 있습니다.

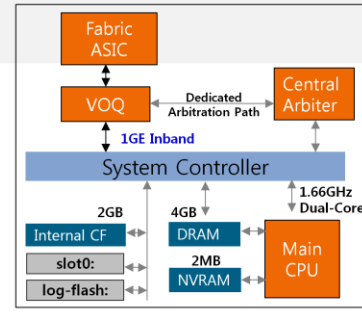
수집, 분석에도 와이어 샤크처럼 많은 필터를 제공하고 있으므로 불필요한 패킷을 걸러내고 필요한 패킷만 분석할 수 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

Tip. Ethanalyzer를 활용한 High CPU 유발 패킷 수집

- High CPU 증상에서 EEM을 활용한 증거파일 수집 방법

```
Nexus7K(config)# event manager applet HIGH-CPU
Nexus7K(config-applet)#   event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type exact entry-op ge entry-val 1 po
ll-interval 1
Nexus7K(config-applet)#   action 1.0 syslog msg High CPU hit $_event_pub_time.
Nexus7K(config-applet)#   action 2.0 cli enable
Nexus7K(config-applet)#   action 3.0 cli show clock >> bootflash:high-cpu.txt
Nexus7K(config-applet)#   action 4.0 cli show proc cpu sort >> bootflash:high-cpu.txt
Nexus7K(config-applet)#   action 5.0 cli ethanalyzer local interface inband limit-captured-frames 10000 >> bootfla
sh:high-cpu-cap.txt

Nexus7K # 2011 Jun 13 09:33:07 switch %$ VDC-1 %$ %EEM_ACTION-6-INFORM: High CPU hit
Nexus7K # dir
       2070    Jun 13 09:35:06 2011  high-cpu-cap.txt
     704247    Jun 13 09:35:06 2011  high-cpu.txt
      16384    Mar 28 20:59:21 2011  lost+found/
```

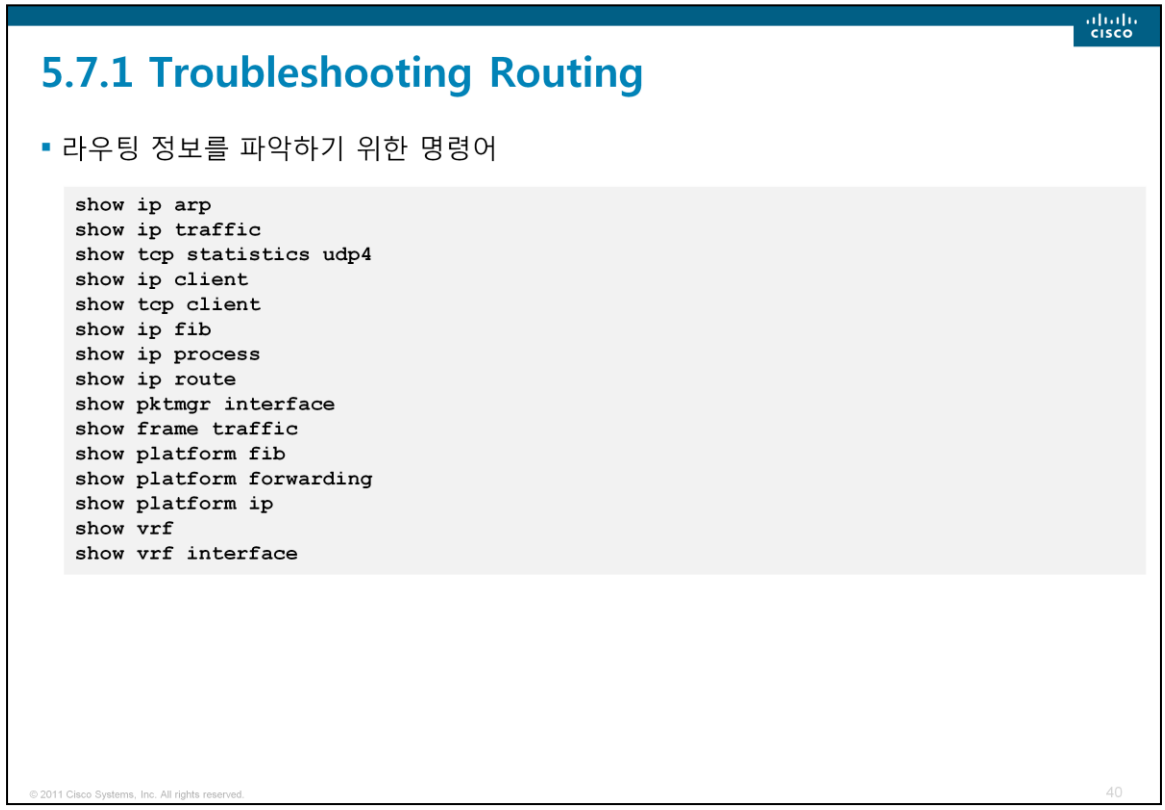


© 2011 Cisco Systems, Inc. All rights reserved.

High CPU utilization 현상은 아주 짧은 시간에 발생해서 사라지는 경우가 많습니다.
이런 경우 NX-OS에서 제공하는 EEM (스크립트)를 활용하여 CPU 가 높은 경우 몇가지 명령어를 실행하여 disk 에 저장할 수 있도록 위와 같이 스크립트를 설정 할 수 있습니다.

이렇게 되면 야간 혹은 짧은 시간에 발생한 High CPU 현상에 대한 실마리 혹은 해결을 할 수도 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



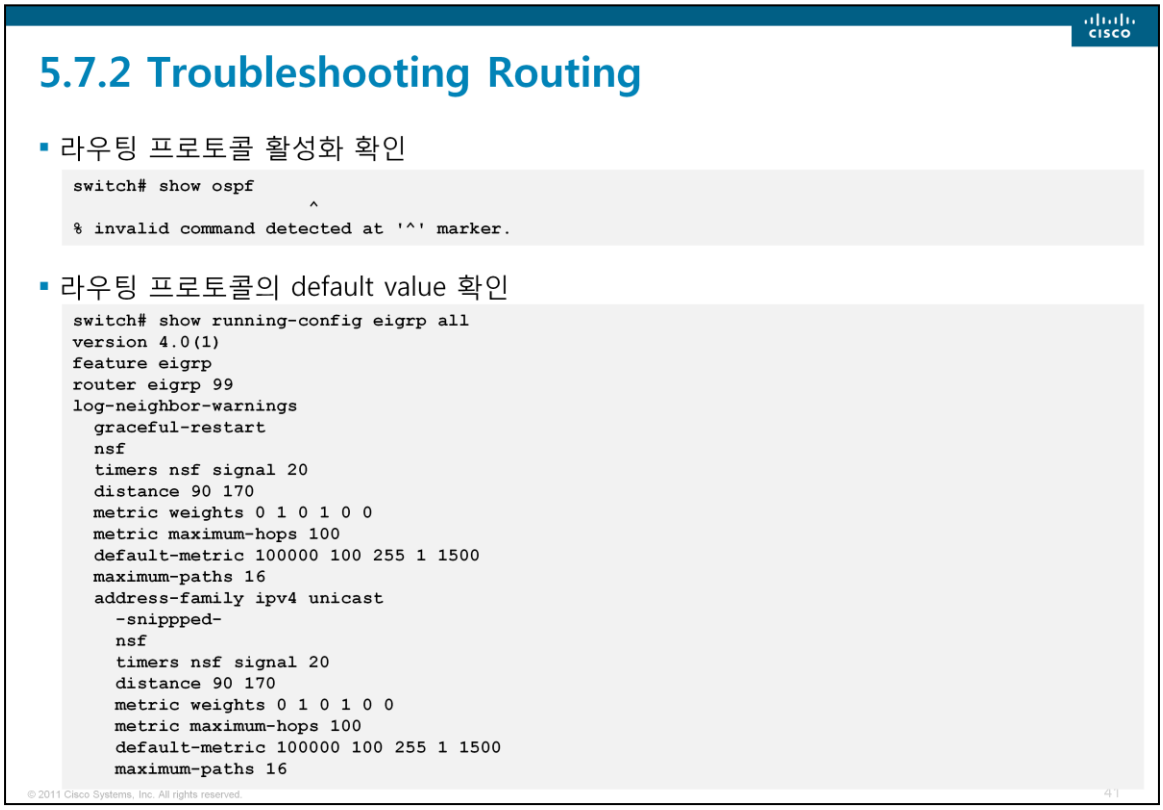
Layer3 라우팅은 optimal routing path와 patch switching을 포함한다. 하나의 라우터에서 목적지까지 가위 위한 optimal path 계산을 위해 라우팅 알고리즘을 사용할 수 있다. 이런 계산은 선택한 라우팅 알로리즘, route metric, 그리고 load balancing 및 alternate path discovery와 같은 기타 요소들에 의존적이다.

NX-OS는 VDC domain 마다 독립된 management를 제공하기 위해서 Virtual device context (VDC)를 사용한다. 각각 VDC는 multiple Virtual routing and forwarding instances (VRFs)를 지원하고 multiple routing information based (RIBs)를 지원한다. 이렇게 함으로써 multiple address domain을 지원할 수 있다. 각각의 VRF는 routing information base (RIB) 과 forwarding information based (FIB)에 의해서 수집된 정보와 묶여져 연동된다.

Layer3 라우팅 이슈에 대해 관련된 자료를 수집할 때 필요한 명령어들은 아래와 같다.

show ip arp
show ip traffic
show tcp statistics udp4
show ip client
show tcp client
show ip fib
show ip process
show ip route
show pktmgr interface
show frame traffic
show platform fib
show platform forwarding
show platform ip
show vrf
show vrf interface

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



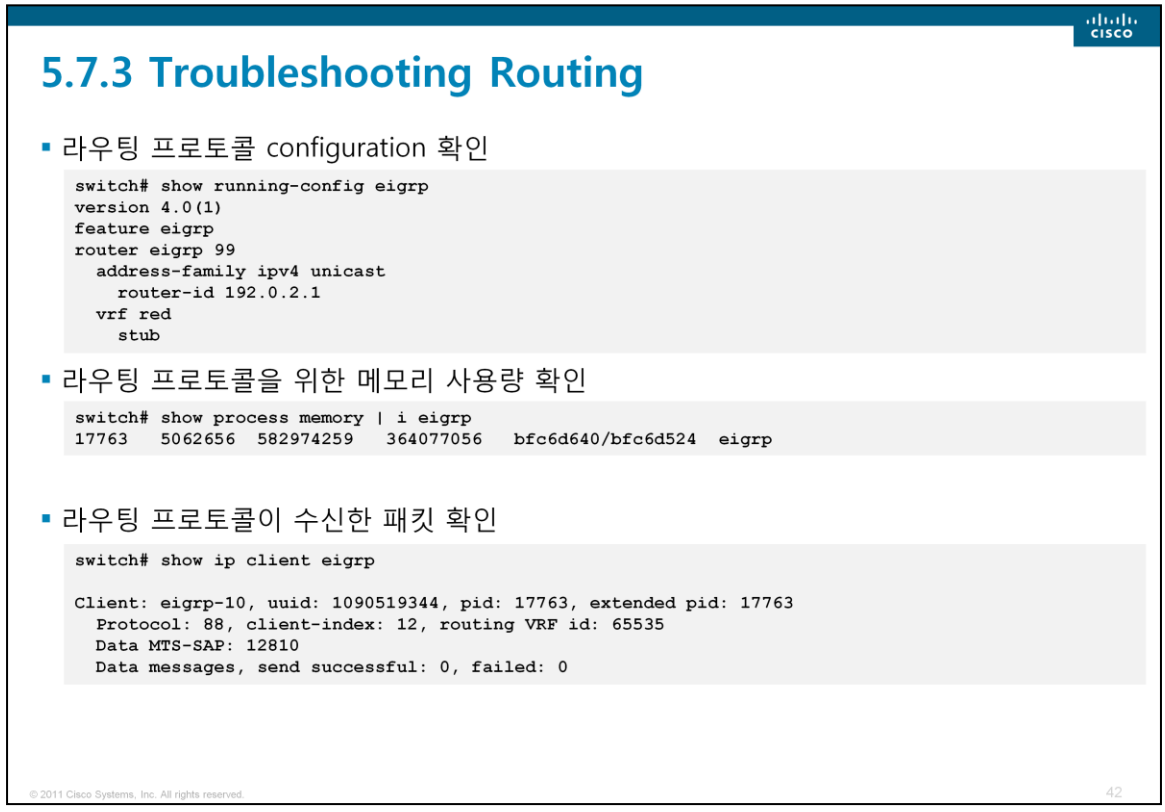
Layer3 라우팅 트러블 슈팅의 가장 기본적인 확인은 위와 같이 해당 라우팅 프로토콜이 enable 되어 있는지 확인하는 것 부터 시작이 됩니다.

switch# show ospf
^
% invalid command detected at '^' marker.

해당 시스템에 ospf feature가 enable 되어 있지 않다면 위와 같은 에러 메시지를 볼 수 있습니다.

NS-OX 명령어 중에서 유용한 명령어가 show running-config [feature name] all 이라는 명령어 입니다.
All 이라는 keyword를 맨 뒤에 붙이게 되면 해당 시스템이 가지고 있는 default 설정을 모두 보여 주게 됩니다.
간혹 default 설정 값이 궁금한 경우 보기가 어려웠는데, 위의 all keyword를 맨 뒤에 붙이시면 쉽게 보실 수 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



사용하는 라우팅 프로토콜 설정을 확인하는 과정이 필요합니다.

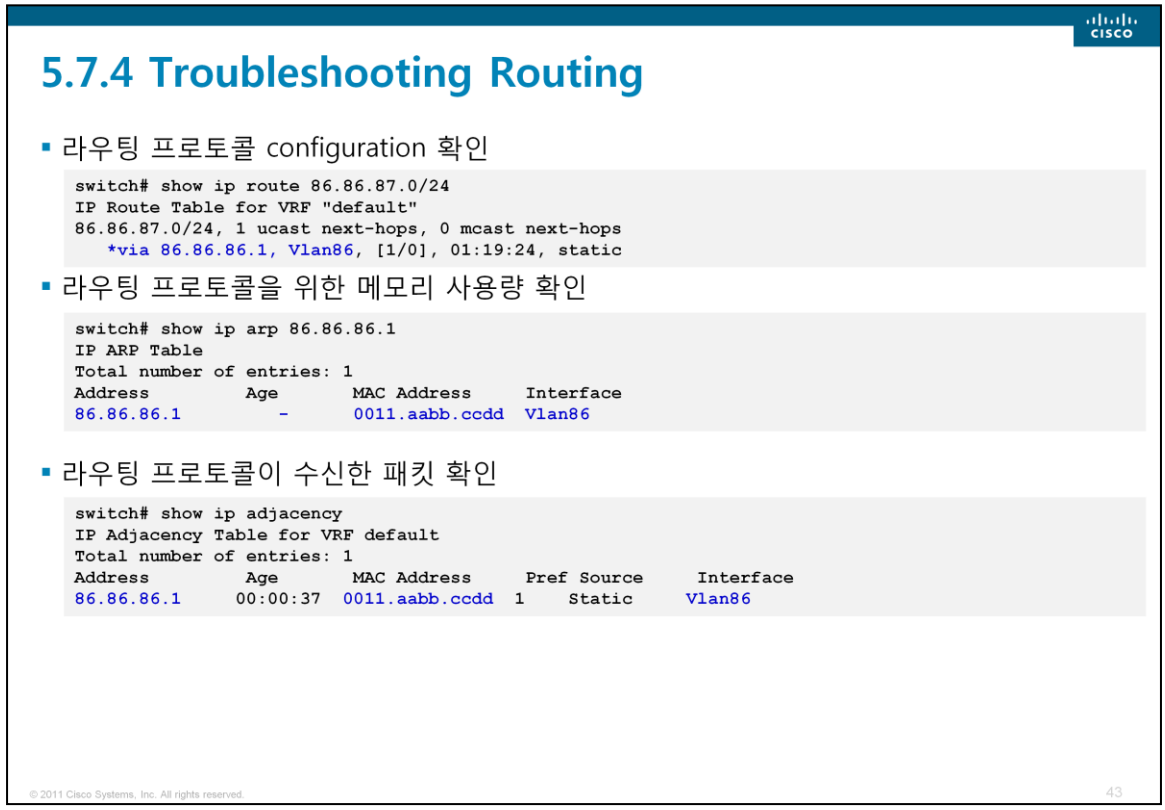
show running-config [feature name]을 입력하시면 해당 feature를 위해 설정된 configuration만 filter를 해서 보여주게 됩니다.

```
switch# show running-config eigrp
version 4.0(1)
feature eigrp
router eigrp 99
  address-family ipv4 unicast
    router-id 192.0.2.1
  vrf red
    stub
```

위에서 전체 configuration 중에서 eigrp 와 연관된 config 만 보고 싶을 때 유용한 명령어 입니다.

또한 추가적으로 위에 보시는 것처럼 라우팅 프로토콜이 사용하는 메모리 사용량 및 라우팅 프로토콜이 송/수신하는 패킷 수 등을 같이 보실 수 있습니다. 라우팅 프로토콜이 상대방 장비와 통신할때는 주기 적으로 해당 카운터가 증가함을 확인해야 합니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



Routed traffic을 위한 Layter3 forwarding

Layer 3 엔진은 라우터를 통화하는 트래픽을 위하여 layer 3 forwarding 만을 수행합니다.
이것 트래픽은 local에서 라우터로 valid한 routed interface의 MAC address로 보내지는 트래픽 입니다.

Routed traffic을 트러블슈팅 하기 위해서는, 다음과 같은 몇 가지를 수행 해야 합니다.

tasks:
1. control plane routing이 올바른지 확인
2. Ingress module의 Hardware forwarding entry의 정보가 일치하는지 확인

Note: 모든 traffic의 라우팅은 ingress module의 forwarding engine에서 수행됩니다.
예를 들어서, 86.86.87.0/24 라우팅을 트러블 슈팅한다고 가정해 보면,
이 네트워크 도달하기 위한 next hop은 86.86.86.1 이고 vlan 86을 통해서 나가도록 설정되어 있습니다.

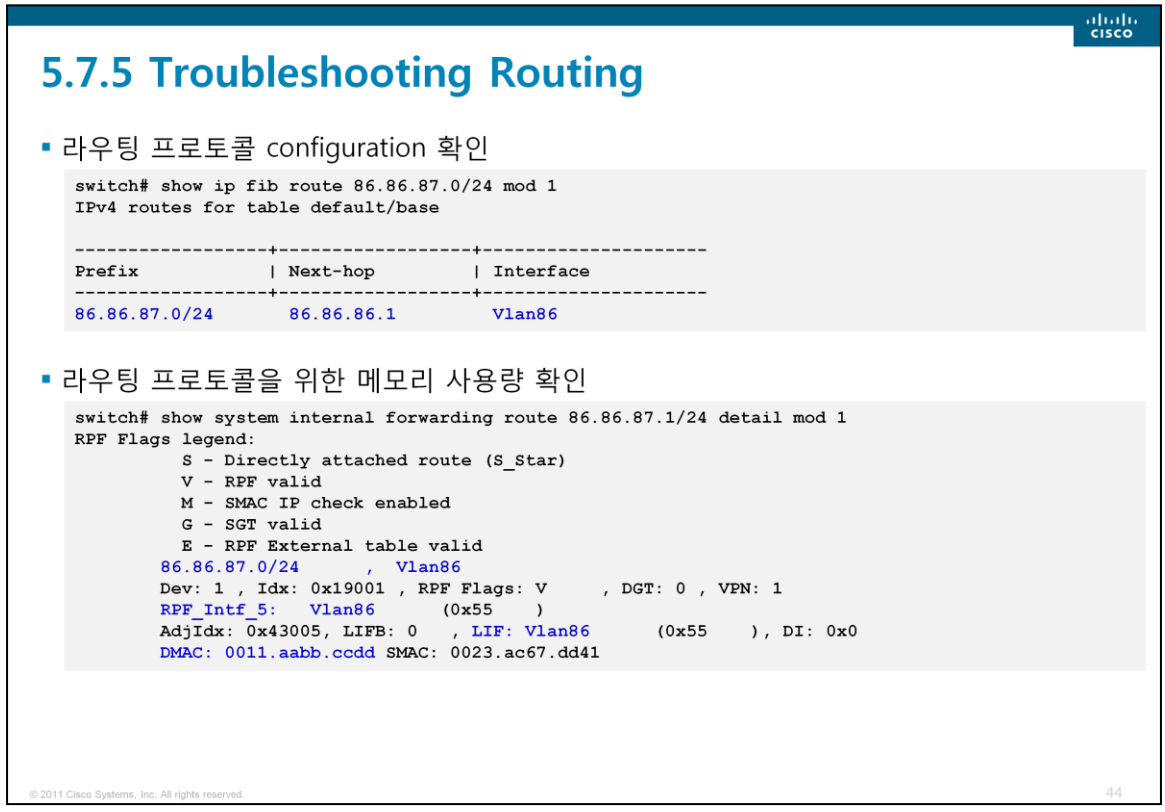
위와 같이 라우팅 테이블을 보고서 위와 같은 정보를 먼저 봐야 합니다.
그리고 그 다음은 next hop으로 가기 위한 ARP가 정확히 associate 되었는지 확인하고 adjacency table에 valid한 adjacency 정보가 있는지도 확인해야 합니다.

우리가 볼 수 있는 것처럼,
86.86.87.0/24 목적지롤 하기 위해서는 86.86.86.1로 route가 잡혀 있고, VLAN 86을 통해서 나가게 됩니다.
그리고 MAC address는 0011.aabb.ccdd 로 association 되어 있습니다.
이 정보는 hardware 정보를 보기 위한 기본 자료가 될 것입니다.

필요한 명령어는 아래와 같습니다.

show ip route (prefix)
show ip arp (nexthop)
show ip adjacency

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



앞 슬라이드 예제는 control plane을 보여 줍니다.
이제 하드웨어 엔트리에 layer 3 hardware 정보를 잘 가지고 있는지 따져봐야 합니다.

위에 보시는 것처럼 IP FIB은 86.86.87.0/24 목적지 prefix 에 대해서 next hop으로 86.86.86.1 정보를 잘 가지고 있습니다.

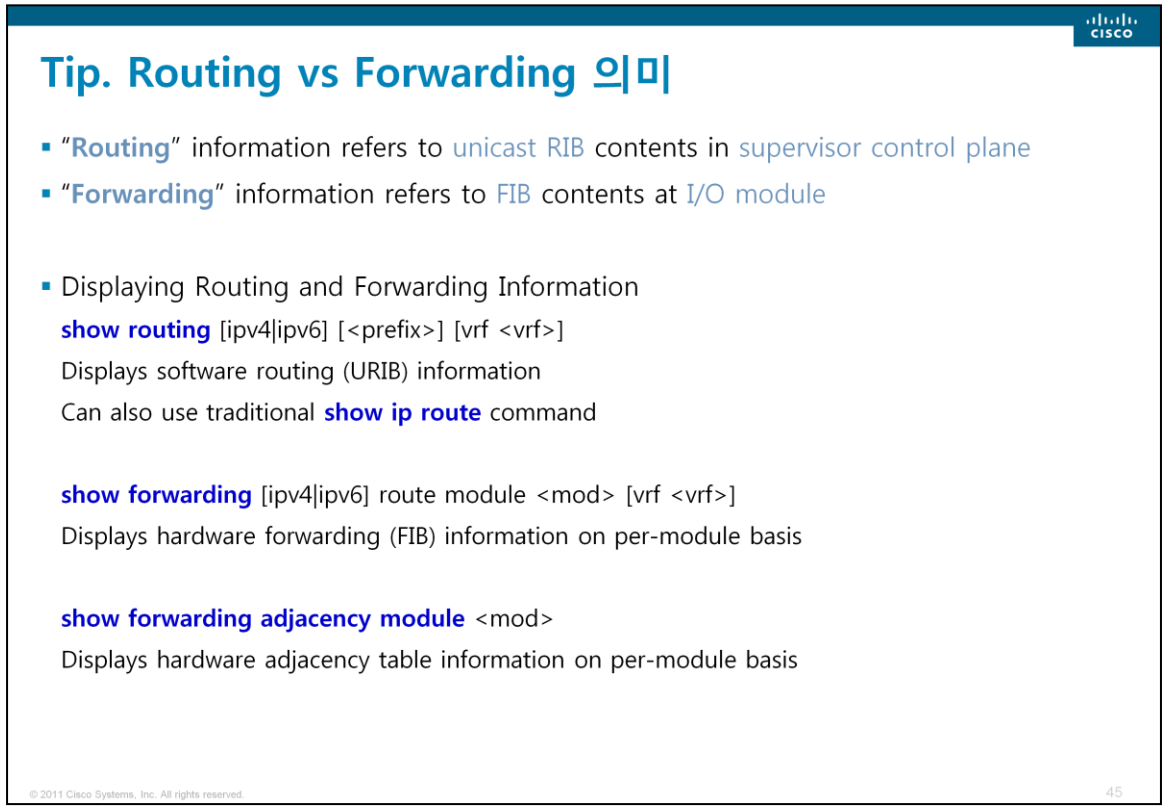
우리가 보는 것처럼 하드웨어 엔트리에서 VLAN86을 통해서 routed out 되는 것을 볼 수 있고 RPF 또한 valid 합니다. (RPF checking을 올렸다면)
그리고 route entry도 MAC 0011.aabb.ccdd와 잘 associate 되어 있습니다.

이것이 의미하는 것은, forwarding plane의 routing이 올바르게 프로그램되어 있고 forwarding이 이 정보를 기반으로 수행된다는 것입니다.

show ip fib route *prefix* **module** *module*
show ip fib route 86.86.87.0/24 mod 1

show system internal forwarding route *prefix* **detail module** *module*

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



Routing 정보는 supervisor control plane에 있는 unicast RIB contents 를 의미합니다.
Forwarding 정보는 I/O module의 FIB contents를 의미 합니다.

따라서 트래픽은 RIB에 의해서 만들어진 라우팅 테이블이 각각의 I/O (라인카드)로 하드웨어 포워딩을 할 수 있는 FIB 테이블로 만들어진 후 이 FIB 정보를 기반으로 하드웨어 포워딩이 되어 지는 것입니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

5.7.6 Troubleshooting Routing

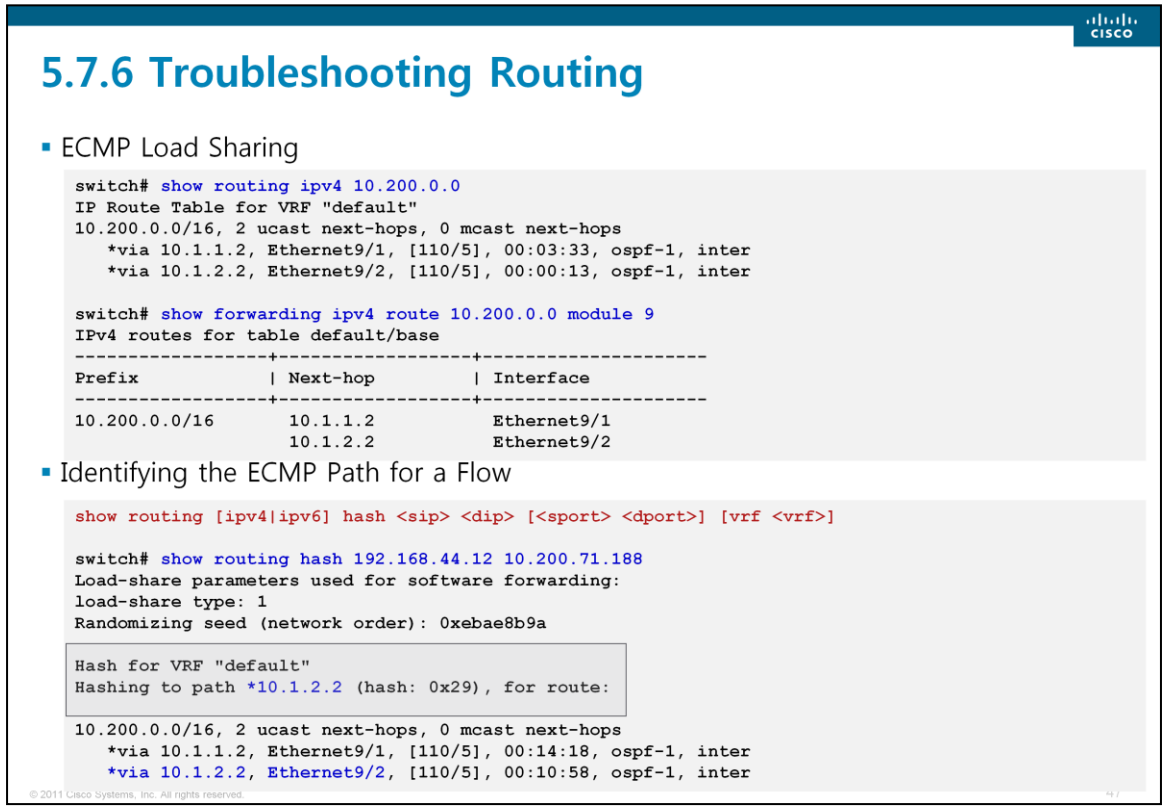
- RIB, FIB, ADJ 테이블 확인

```
switch# show routing ipv4 10.100.7.0/24
IP Route Table for VRF "default"
10.100.7.0/24, 1 ucast next-hops, 0 mcast next-hops
   *via 10.1.2.2, Ethernet9/2, [110/5], 00:02:30, ospf-1, type-1

switch# show forwarding ipv4 route 10.100.7.0/24 module 9
IPv4 routes for table default/base
------------------+------------------+---------------------
Prefix            | Next-hop         | Interface
------------------+------------------+---------------------
10.100.7.0/24       10.1.2.2           Ethernet9/2

switch# show forwarding adjacency 10.1.2.2 module 9
IPv4 adjacency information, adjacency count 1
next-hop          rewrite info    interface
---------------  --------------  ----------
10.1.2.2          0010.9400.0001  Ethernet9/2
```

© 2011 Cisco Systems, Inc. All rights reserved.

RIB 정보와 FIB 정보를 확인 할 수 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



이번 슬라이드는 ECMP (Equal Cost Multi-Path)를 RIB, FIB 정보를 이용해서 확인하는 방법을 예로 보여드립니다.

RIB 테이블의 정보로 보면, 목적지 10.200.0.0은 두개의 neighbor로 부터 동일한 cost로 테이블에 보여집니다. 즉, 두 경로를 통해서 해당 목적지에 도달할 수 있으므로 flow 별로 LB를 태워서 패킷을 보내게 될 것 입니다. 그러나 문제는 두 경로 중에서 정확히 어떤 경로를 타는지 알 수 없다는 것입니다.

물론 FIB 테이블 보더라도 조금 더 직관적으로 보이기는 하나 어떤 경로를 통해서 나가는 것은 확인 할 수 없습니다. 단지 하드웨어 포워딩을 할 준비가 되어 있다는 것을 알 수 있습니다.

이때 아래와 같은 명령어로 source ip와 destination ip를 넣어서 시뮬레이션을 해 볼 수 있습니다.

show routing [ipv4|ipv6] hash <sip> <dip> [<sport> <dport>] [vrf <vrf>]
show routing hash 192.168.44.12 10.200.71.188

실제 시뮬레이션 결과 아래처럼 10.1.2.2에 *가 붙은 것을 볼 수 있습니다.

```
Hashing to path *10.1.2.2 (hash: 0x29), for route:
```

즉, 두 개의 next hop 중에서 10.1.2.2 쪽으로 위의 트래픽이 나가는 것을 볼 수 있습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

Tip. ARP, Mac aging 비교

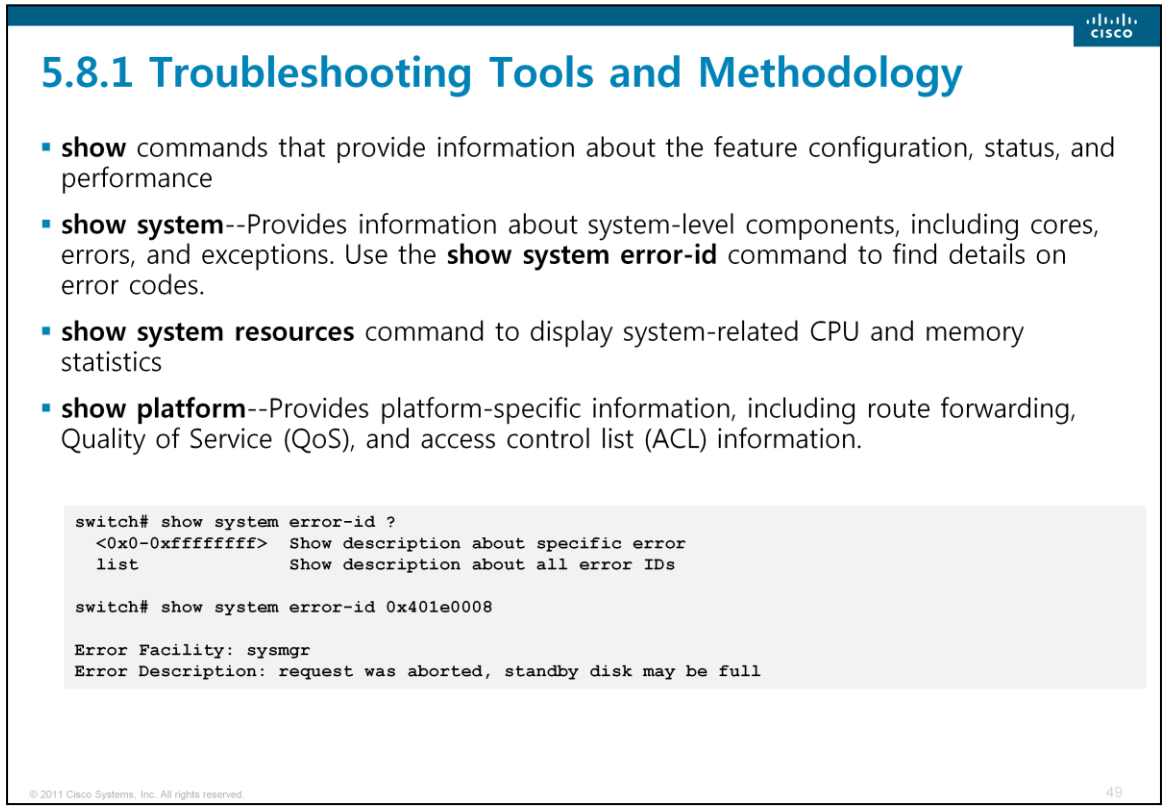
- IOS와 NX-OS간 Mac, ARP 동작 비교

	IOS	NX-OS
ARP age out	4 hours (14400 seconds)	25 minutes (1500 seconds)
Mac age out	5 minutes (300 seconds)	30 minutes (1800 seconds)
ARP age out전 behavior	60 sec 전 unicast arp를 host에 전송 응답 오면 : arp entry update 응답 안오면 : 60 sec 후 재전송 응답 안오면 : arp entry 삭제	
clear ip arp	unicast arp 전송	
refresh ARP 방식	unicast 방식	broadcast 방식 주기적인 broadcast arp packet (대략 1500 sec)
Mac sync process	FF 존재Earl간의 H/W Sync 기능 없음 (software-sync 기능 없음)	FF 존재 (Flood to Fabric)Earl간의 l2fm 에서 수행 (software-sync 기능-즉시)
MM(mac notification)	MM 사용 Flooding은 MM 받거나 mac-sync 설정 되면 없어진다.	사용하지 않음

© 2011 Cisco Systems, Inc. All rights reserved.

이번 슬라이드는 기존 Catalyst 6500의 IOS와 Nexus 700의 NX-OS에 구현된 차이점 중에서 MAC 과 ARP를 핸들링하는 차이에 대해서 정리해 보았습니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.



문제 해결을 위해서 CLI 에서 show 명령어를 많이 사용하게 됩니다.

show 명령어는 feature configuration, status, performance 등 과 관련된 정보를 제공 합니다.
또한 뒤에 나오는 몇 가지 명령어 카테고리를 사용하면 추가적인 정보를 함께 얻을 수 있습니다.

show system : system-level component 예를 들어, core, error, exception 에 관한 정보를 제공합니다.
show system error-id 명령어는 error code에 대한 상세한 내용을 제공 합니다.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

Tip. Basic Command

- **Link flap**

  From Sup:
  show logging
  show tech module <mod#>
  show tech ethpm
  show hardware internal phy event-history port <port#>

- **vPC**

  show running-config vpc
  show vpc consistency-parameters interface
  show vpc
  show vpc peer-keepalive
  show vpc consistency-parameters
  show vpc statistics [peer-link | peer-keepalive | vpc #]
  show system internal vpcm event-history [errors | msgs | interactions]

© 2011 Cisco Systems, Inc. All rights reserved.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

Tip. Basic Command

- **Port-channel**

  From Sup:
  show logging
  show tech lacp all
  show tech ethpm
  show system internal pktmgr interface port-channel X
  show system internal eltm info interface port-channel X
  show system internal ethpm info interface X
  show port-channel internal event-history [all | lock | msgs | errors]
  show lacp internal event-history interface x

- **Module reset**

  From Sup:
  show logging
  show tech module X

  From Module:
  show logging onboard obfl-history
  show logging onboard kernel-trace
  show logging onboard exception-log
  show logging onboard boot-uptime
  All "show logging onboard" commands can be used for Sup reset also.

© 2011 Cisco Systems, Inc. All rights reserved.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

Tip. Basic Command

- 모듈 관련 이슈

```
show module
show logging nvram

show system reset-reason
show system reset-reason module <x>

show module internal event-history module <x>
show module internal activity module <x>
show module internal exception-log module <x>
show module internal event-history errors

show tech-support details
show tech-support platform
show tech-support internal module <x>
```

© 2011 Cisco Systems, Inc. All rights reserved.

All contents are Copyright © 1992–2011 Cisco Systems, Inc.
All rights reserved. Cisco Korea TAC.

소속 : Cisco Korea TAC
작성자 : 윤치권 (chyoon@cisco.com)
작성일 : 2012. 06. 20
버전 : version 3.2

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. Cisco Korea TAC.