Konvergence pevných a bezdrátových sítí: řešení a produkty

T-NET2 / L2

Radek Boch, CCIE# 7095, Systems Engineer Cisco
Pavel Minařík, Invea-Tech
Agenda

Catalyst 3850 – Overview
  Catalyst 3850 – Platform Architecture
  Catalyst 3850 – Stacking Architecture
  Catalyst 3850 – High Availability
  Catalyst 3850 – QoS
  Catalyst 3850 – Flexible NetFlow
  Catalyst 3850 – Key Takeaways
Evolving User Workspace - Megatrends

**Deliver an Uncompromised User Experience on Any Workspace**

**IT Requirement**

**BYOD**
- Secure access
- Customized experience
- Guest access

**Mobility**
- Seamless roaming
- Optimal client performance
- Cloud access/VXI

**Video**
- Multicast streaming
- Video conferencing
- Reliable performance
Single Platform for Wired and Wireless

**Benefits**
- Built on **UADP ASIC** – Cisco’s Innovative Flexparser ASIC technology
- Eliminates operational complexity
- Single Operating System for wired and wireless

**Features:**
- 802.11n
- CleanAir
- VideoStream
- Radio Resource Management (RRM)
- Wireless Intrusion Prevention System (WiPS)
- 802.11ac Ready

**Features:**
- Stacking
- Stackpower
- Flexible Netflow
- Granular QoS
- Trustsec*/Identity
- AVC/Medianet*
- Smart Operations*
- EnergyWise*

Note: All features may not be available on new platforms at introduction but are expected to be added within 12-18 months.
Evolution of Converged Access

INTEGRATED CONTROLLER OPTIONS

DMZ
Prime
ISE

INTEGRATED MOBILITY CONTROLLER

WAN

BRANCH
CAT 3850
Employee
Guest

SMALL/MEDIUM CAMPUS
New Catalyst 3850
Integrated Mobility Controller
Integrated Mobility Controller
Access Points
AP CAPWAP Tunnels

UP TO 50 ACCESS POINTS
UP TO 2,000 CLIENTS
ALL WAN SERVICES AVAILABLE

UP TO 250 ACCESS POINTS
UP TO 16,000 CLIENTS
VISIBILITY, CONTROL, RESILIENCY

EXTERNAL MOBILITY CONTROLLER NEEDED

ISE
Prime

5508 or WISM2 with SW Upgrade or new 5760

LARGE CAMPUS
New Catalyst 3850
Mobility Agent
Catalyst 3750
Access Points

UP TO 72,000 ACCESS POINTS
UP TO 864,000 CLIENTS
LARGEST LAYER 3 ROAMING DOMAINS

Capwap Tunnel
Standard Ethernet, No Tunnels
Guest Tunnel from Switch to DMZ Controller
Converged Wired / Wireless Access – Benefits … Overview

Single platform for wired and wireless
Common IOS, same administration point, one release

Network wide visibility for faster troubleshooting
Wired and wireless traffic visible at every hop

Consistent security and quality of service control
Hierarchical bandwidth management and distributed policy enforcement

Maximum resiliency with fast stateful recovery
Layered network high availability design with stateful switchover

Scale with distributed wired and wireless data plane
480G stack bandwidth; 40G wireless / switch; efficient multicast; 802.11ac fully ready

Unified Access - One Policy | One Management | One Network
Built on Cisco’s Innovative “UADP” ASIC

- Wireless CAPWAP Termination
- Integrated Controller: Up to 50 APs
- Up to 2000 Clients per Stack
- 40 Gbps Uplink Bandwidth
- Stackpower
- Line Rate on All Ports
  - Two versions:
    - 24 ports
    - 48 ports
- 480 Gbps Stacking Bandwidth
- Full POE+
- FRU Fans, Power Supplies
- Granular QoS/Flexible NetFlow
Catalyst 3850 Highlights

Integrated Wireless LAN Functionality
- Common features across wired and wireless

New differentiated services
- IOS XE – Extensible Modular Operating System
- Flexible Netflow
- Granular QoS
- TrustSec*
- SDN Ready (OnePK and Openflow)

Best-in-class stackable switch
- Performance – Line rate 480G Stackwise Technology
- Full POE+ support, UPOE option*
- Modular Network Modules – up to 4x10G
- High Availability with Stack SSO and StackPower
- Multi-core CPU
- EEE
- Unified Access Data Plane (UADP) ASIC

* Roadmap
Catalyst 3850 – Wireless Capabilities

- CAPWAP termination and DTLS in Hardware
- 40G wireless capacity/switch
  - Capacity increases with members
- 50 APs and 2000 clients/switch stack
- Wireless switch peer group support for faster roaming: latency sensitive applications
- Supports IPv4 and IPv6 client mobility
- AP’s must be directly connected to Catalyst 3850
- Requires IP Base license level for Wireless functionality

Best-in-Class Wired Switch – with Integrated Wireless Mobility functionality
Network Modules

WS-C3850-NM-4-1G
- 4 x 1G
- SFP
- Supported on WS-C3850-24 & WS-C3850-48 Port

WS-C3850-NM-2-10G
- 4 x 1G OR 2 x 10G
- OR 2 x 1G + 1 x 10G
- SFP & SFP+
- Supported on WS-C3850-24 & WS-C3850-48 Port

WS-C3850-NM-4-10G
- Auto-sensing – All Combinations
- SFP & SFP+
- Supported on WS-C3850-48 only
Catalyst 3850
Power Modules

<table>
<thead>
<tr>
<th>PWR Modules</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR-C1-350WAC</td>
<td></td>
</tr>
<tr>
<td>PWR-C1-715WAC</td>
<td></td>
</tr>
<tr>
<td>PWR-C1-1100WAC</td>
<td></td>
</tr>
<tr>
<td>PWR-C1-440WDC</td>
<td></td>
</tr>
</tbody>
</table>

- Power Modules is same as 3K but with a new PID
- Classic 3K Power Module can work on Catalyst 3850s
- No Interworking with classic 3Ks for StackPower
Catalyst 3850 – Stacking Cable

Stacking Cable

3 Rings going East

Stacking Cable Connectors

3 Connectors going East

Stacking Cables
**IOS-XE – Evolution**

- Modern IOS to enable multi-core CPU
- Easy customer migration
- While maintaining IOS functionality and look and feel
- Allow hosted applications like Wireshark

**IOS 12.2(52)SE**

**IOS**
- Features Components
- Common Infrastructure / HA
- Management Interface
- Module Drivers
- Kernel

**IOSd**
- Features Components

**Hosted Apps**
- WCM

**IOS XE version 3.2.0 SE**
**IOSd version 15.0(1) EX**
Agenda

- Catalyst 3850 – Overview
- **Catalyst 3850 – Platform Architecture**
  - Catalyst 3850 – Stacking Architecture
  - Catalyst 3850 – High Availability
  - Catalyst 3850 – QoS
  - Catalyst 3850 – Flexible NetFlow
- Catalyst 3850 – Key Takeaways
### Improved Hardware Resources

TCAM/HASH availability for L2, L3, ACEs, Multicast for IPv4

<table>
<thead>
<tr>
<th>Field</th>
<th>Catalyst 3750X</th>
<th>Catalyst 3850</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC addresses</td>
<td>4k</td>
<td>32k</td>
</tr>
<tr>
<td>Unicast Routes*</td>
<td>6k</td>
<td>24k</td>
</tr>
<tr>
<td>IGMP Groups and Multicast routes</td>
<td>1k</td>
<td>8k</td>
</tr>
<tr>
<td>Security ACEs</td>
<td>2k</td>
<td>3k</td>
</tr>
<tr>
<td>QOS ACEs</td>
<td>0.5k</td>
<td>2.8k</td>
</tr>
<tr>
<td>PBR ACEs</td>
<td>0.5k</td>
<td>1.2k</td>
</tr>
</tbody>
</table>

IPv6 consumes 2 entries in the look-up table

* - in the HASH

Comparing “Access” SDM template on 3750x with “Advanced” SDM template on 3850
## Catalyst 3750-X and Catalyst 3850

<table>
<thead>
<tr>
<th>Features</th>
<th>Catalyst 3750-X</th>
<th>Catalyst 3850</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacking</td>
<td>64 Gbps</td>
<td>480 Gbps</td>
</tr>
<tr>
<td>IOS Wireless Controller</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Queues per Port</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>QOS Model</td>
<td>MLS</td>
<td>MQC</td>
</tr>
<tr>
<td>Uplinks</td>
<td>2 x 10 Gbps</td>
<td>4 x 10 Gbps</td>
</tr>
<tr>
<td>Buffers</td>
<td>6MB/48 port model</td>
<td>12MB/48 port model</td>
</tr>
<tr>
<td>Stackpower</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Native Flexible Netflow Support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Multi-Core CPU for Hosted Services</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Flash Size</td>
<td>64 Mb</td>
<td>2 Gb</td>
</tr>
<tr>
<td>Operating System</td>
<td>IOS on 15.0 release train</td>
<td>IOS-XE on 15.0 release train</td>
</tr>
</tbody>
</table>
Catalyst 3850 – Inside View

- PoE+ Controllers (x2)
- UADP ASICs
- Stack Power Controller
- Power Stack Conn (x2)
- Redundant Power Supplies
- Downlink Phys (x6)
- Fan FRU (x3)
- Back Stack Conn (x2)
- Ethernet And Console Port
- FRU Uplink Module
- Cavium CPU
Catalyst 3850 –
WS-C3850-24 Layout

480G STACK INTERFACE

Packet Buffer

Forwarding Controller

Network Interface

800 MHz Quad-Core CPU

FPGA

DRAM 4GB

Flash 2GB

USB

Ingress FIFO

Egress FIFO

Reassembly Crypto

Octal PHY MACSec

Octal PHY MACSec

Octal PHY MACSec

Dual PHY MACSec

Dual PHY MACSec

24 Port PoE+

24 x 1G 10/100/1000

2 x 10G, 2 x 1G / 4 x 1G

EMP

Console

Network Interface

Packet Buffer

Forwarding Controller

480G STACK INTERFACE

© 2013 Cisco and/or its affiliates. All rights reserved. Cisco Public
Agenda

Catalyst 3850 – Overview
Catalyst 3850 – Platform Architecture
Catalyst 3850 – Stack Architecture
Catalyst 3850 – High Availability
Catalyst 3850 – QoS
Catalyst 3850 – Flexible NetFlow
Catalyst 3850 – Key Takeaways
• Improved Stacking – 480G Bandwidth
  • Each stack port has 3 channels of 80 Gbps each. 2 stack ports = 480 Gbps
  • Uses similar stacking algorithm as 3750X (destination strip)
  • Supports auto-upgrade of IOS images in a stack (like 3750X)

• 4 Member stack support at FCS
  • 9 member stack support in SW roadmap*
  • Based on IOS HA - SSO
  • No backward compatibility with 3750 series

• StackPower for Power redundancy
  • Identical to 3750X

* Roadmap
Catalyst 3850
Understanding the Stack Ring

- 6 rings in total
- 3 rings go East
- 3 rings go West
- Each ring is 40G
- Total Stack BW – 240G
- With Spatial Reuse= 480G

Stack Interface of UADP

Assuming 4 x 24-port 3850 Switches

Stack Interface of UADP

Packets are segmented/reassembled in HW (256 byte segments)
Catalyst 3850

Unicast Packet Path

Assuming 4 x 24-port 3850 Switches

Destination Stripping
Packet travels 1/2 the rings.
Taken out of stack by destination

Creating Segments

Re-ordering segments
Catalyst 3850

Unicast Packet Path – Spatial Reuse

Assuming
4 x 24-port
3850 Switches

Destination
Stripping
Packet travels ½
the rings.
Taken out of stack
by destination
Catalyst 3850
Multicast Packet Path on the Stack Ring

Assuming 4 x 24-port 3850 Switches

Source Stripping Packet travels the full rings Taken out by source, when packet reach back
Catalyst 3850
Stack Ring Healing

Example shows:
4 x 24-port
3850 Switches
Catalyst 3850

Stack Ring Healing

Example shows:
4 x 24-port
3850 Switches

Failure:
Detection is by hardware
Software is notified immediately
Ring Wrap initiated immediately > 1 ms
Catalyst 3850
Stack Ring Healing

Example shows: 4 x 24-port 3850 Switches

Failure:
Detection is by hardware
Software is notified immediately
Ring Wrap initiated immediately > 1 ms

Recovery:
Hardware detects other side
Software validates the link and so it brings up the connection gracefully

Unwrap is slower than Wrap
Agenda

Catalyst 3850 – Overview
Catalyst 3850 – Platform Architecture
Catalyst 3850 – Stacking Architecture

Catalyst 3850 – High Availability
Catalyst 3850 – QoS
Catalyst 3850 – Flexible NetFlow
Catalyst 3850 – Key Takeaways
Catalyst 3850
HA Redundancy – Shift from 3750-X

Catalyst 3750-X – StackWise-Plus
- Hybrid control-plane processing
- N:1 stateless control-plane redundancy
- Distributed L2/L3 Forwarding Redundancy
- Stateless L3 protocol Redundancy

Catalyst 3850 – StackWise-480
- Centralized control-plane processing
- 1+1 Stateful redundancy (SSO)
- Distributed L2/L3 Forwarding Redundancy
- IOS HA Framework alignment for L3 protocol
**Catalyst 3850**

Stacking, vs. Catalyst 6500

- Active and Standby Members run IOSd, WCM, etc.
- Synchronize information
- Active controls Data plane programming for all members
- Member switches act as Line cards – connected via the Stack Cable

- Active and Standby Supervisors
- Run IOS on Supervisors
- Synchronize information
- Active programs all DFCs
- DFCs run a subset of IOS for LCs
Catalyst 3850
Stack Discovery

- Switches boot
- Stack Interfaces brought online
- Infra and LC Domains boot in parallel
- Stack Discovery Protocol discovers Stack topology
- In full ring, discovery exits after all members are found
- In an incomplete ring, system waits for 2mins
- Active Election begins after Discovery exits
- Election based on Highest Priority OR Lower MAC
Catalyst 3850
Stack Formation
Catalyst 3850

Stack Formation

• Active starts RP Domain (IOSd, WCM, etc) locally
Catalyst 3850

Stack Formation

• Active starts RP Domain (IOSd, WCM, etc) locally
• Programs hardware on all LC Domains
• Traffic resumes once hardware is programmed
• Starts 2min Timer to elect Standby in parallel
Catalyst 3850

Stack Formation

• Active starts RP Domain (IOSd, WCM, etc) locally
• Programs hardware on all LC Domains
• Traffic resumes once hardware is programmed
• Starts 2min Timer to elect Standby in parallel
• Active elects Standby
• Standby starts RP Domain locally
Catalyst 3850

Stack Formation

• Active starts RP Domain (IOSd, WCM, etc) locally
• Programs hardware on all LC Domains
• Traffic resumes once hardware is programmed
• Starts 2min Timer to elect Standby in parallel
• Active elects Standby
• Standby starts RP Domain locally
• Starts Bulk Sync with Active RP
Catalyst 3850

Stack Formation

• Active starts RP Domain (IOSd, WCM, etc) locally
• Programs hardware on all LC Domains
• Traffic resumes once hardware is programmed
• Starts 2min Timer to elect Standby in parallel
• Active elects Standby
• Standby starts RP Domain locally
• Starts Bulk Sync with Active RP
• Standby reaches “Standby Hot”
Catalyst 3850
Stack Member Addition
Catalyst 3850
Stack Member Addition

- Stack discovery initiated and completed
- Plug in the member, completing full ring
- Power up the member
Catalyst 3850
Stack Member Addition

- Stack discovery initiated and completed
- Plug in the member, completing full ring
- Power up the member
- Stack Discovery process runs and completes immediately after discovery happens
Catalyst 3850
Stack Member Addition

- Stack discovery initiated and completed
- Plug in the member, completing full ring
- Power up the member
- Stack Discovery process runs and completes immediately after discovery happens
- Active detects the new addition, and programs the hardware of the member
- Active is not pre-empted by powering on another member even if it was High Priority
Catalyst 3850
Stack Member Deletion
Catalyst 3850

Stack Member Deletion

- Stack discovery initiated and completed
- Active detects member removal – and Clean up process is initiated
- Clean-up involves removing TCAM entries referencing removed member, MAC addresses, CDP tables – more like all ports on the member are shutdown
- Half Ring
Agenda

Catalyst 3850 – Overview
Catalyst 3850 – Platform Architecture
Catalyst 3850 – Stacking Architecture
Catalyst 3850 – High Availability

Catalyst 3850 – QoS
Catalyst 3850 – Flexible NetFlow
Catalyst 3850 – Key Takeaways
QoS – What’s New with Converged Access

**Wired (Cat 3850)**

- **Modular QoS based CLI (MQC)**
  - Alignment with 4500E series (Sup6, Sup7)
  - Class-based Queueing, Policing, Shaping, Marking

- **More Queues**
  - Up to 2P6Q3T queuing capabilities
  - Standard 3750 provides 1P3Q3T
  - Not limited to 2 queue-sets
  - Flexible MQC Provisioning abstracts queuing hardware

**Wireless (Cat 3850 & CT 5760)**

- **Granular QoS control at the wireless edge**
  - Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network

- **Enhanced Bandwidth Management**
  - Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic

- **Wireless Specific Interface Control**
  - Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  - AAA support for dynamic Client based QoS and Security policies

- **Per SSID Bandwidth Management**

*** NOT available on CT 5760 at FCS
QoS – What’s New with Converged Access

- **Modular QoS based CLI**
  - Alignment with 4500E series (Sup6, Sup7)
  - Class-based Queueing, Policing, Shaping, Marking

- **More Queues**
  - Up to 2P6Q3T queuing capabilities
  - Standard 3750 provides 1P3Q3T
  - Not limited to 2 queue-sets

- **Flexible MQC Provisioning**
  - Abstracts queuing hardware

- **Wired (Cat 3850)**
  - Wireless (Cat 3850 & CT 5760)

- **DMZ**
  - ISE
  - Prime

- **Remote BRANCH**
  - WAN

- **Integrated Controller**
  - UA 3850
  - Employee
  - Guest

**Wireless (Cat 3850 & CT 5760)**

- **Granular QoS control at the wireless edge**
  - Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network

- **Enhanced Bandwidth Management**
  - Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic

- **Wireless Specific Interface Control**
  - Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  - AAA support for dynamic Client based QoS and Security policies

- **Per SSID Bandwidth Management**

*** **NOT available on CT 5760 at FCS**
QoS – What’s New with Converged Access

**With the CT 5760 or CAT 3850**
Usage based fair allocation *without* configuration

**Wireless (Cat 3850 & CT 5760)**

- **Granular QoS control at the wireless edge**
  Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network.

- **Enhanced Bandwidth Management**
  Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic.

- **Wireless Specific Interface Control**
  Policing capabilities Per-SSID, Per-Client upstream*** and downstream.
  AAA support for dynamic Client based QoS and Security policies.

- **Per SSID Bandwidth Management**

---

Max bandwidth allowed: $54 - (4 \times 5) = 34\text{Mbps}$

*** NOT available on CT 5760 at FCS
QoS – What’s New with Converged Access

With the 3850
Bidirectional policing at the edge per-user, per-SSID and in Hardware

Wireless (Cat 3850 & CT 5760)

• Granular QoS control at the wireless edge
  Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network

• Enhanced Bandwidth Management
  Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic

• Wireless Specific Interface Control
  Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  AAA support for dynamic Client based QoS and Security policies

• Per SSID Bandwidth Management

*** NOT available on CT 5760 at FCS

- SSID: BYOD
- QoS policy on 3850 used to police each client bidirectionally
- Policy can be sent via AAA to provide specific per-client policy
- Allocate Bandwidth or police/shape SSID as a whole
QoS – What’s New with Converged Access

With the CT 5760 or CAT 3850
Deterministic bandwidth is allocated per SSID

- Modular QoS based CLI
- Alignment with 4500E series (Sup6, Sup7)
- Class-based Queueing, Policing, Shaping, Marking
- More Queues
  - Up to 2P6Q3T queuing capabilities
  - Standard 3750 provides 1P3Q3T
  - Not limited to 2 queue-sets
- Flexible MQC Provisioning abstracts queuing hardware

Wired (Cat 3850)
Wireless (Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge
  Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network
- Enhanced Bandwidth Management
  Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic
- Wireless Specific Interface Control
  Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  AAA support for dynamic Client based QoS and Security policies
- Per SSID Bandwidth Management

*** NOT available on CT 5760 at FCS
QoS – What’s New with Converged Access

Wired (Cat 3850)

- **Modular QoS based CLI (MQC)**
  - Alignment with 4500E series (Sup6, Sup7)
  - Class-based Queueing, Policing, Shaping, Marking
- **More Queues**
  - Up to 2P6Q3T queuing capabilities
  - Standard 3750 provides 1P3Q3T
  - Not limited to 2 queue-sets
  - Flexible MQC Provisioning abstracts queuing hardware

Wireless (Cat 3850 & CT 5760)

- **Granular QoS control at the wireless edge**
  - Tunnel termination allows customers to provide QoS treatment per SSIDs, per-
    - Clients
  - Flexible MQC Provisioning abstracts queuing hardware

- **Enhanced Bandwidth Management**
  - AFD Bandwidth Management ensures fairness at Client, SSID and Radio levels
  - Per SSID bandwidth allocation

- **Wireless Specific Interface Control**
  - Policing capabilities Per SSID, Per Client upstream and downstream

- **AAA support for dynamic Client based QoS and Security policies**

- **Per SSID bandwidth allocation**

---

**Policy-map PER-PORT-POLICING**

```
Class VOIP
  set dscp ef
  police 128000 conform-action transmit exceed-action drop

Class VIDEO
  set dscp cs4
  police 384000 conform-action transmit exceed-action drop

Class SIGNALING
  set dscp cs3
  police 32000 conform-action transmit exceed-action drop

Class TRANSACTIONAL-DATA
  set dscp af21

Class class-default
  set dscp default
```

*** **NOT** available on CT 5760 at FCS ***
QoS – What’s New with Converged Access

**Wired (Cat 3850)**

- Modular QoS based CLI (MQC)
  Alignment with 4500E series (Sup6, Sup7)
  Class-based Queueing, Policing, Shaping, Marking

- More Queues
  Up to 2P6Q3T queuing capabilities
  Standard 3750 provides 1P3Q3T
  Not limited to 2 queue-sets
  Flexible MQC Provisioning abstracts queuing hardware

**Wireless (Cat 3850 & CT 5760)**

- Granular QoS control at the wireless edge
  Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients

- Enhanced Bandwidth Management
  AFD Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic

- Wireless Specific Interface Control
  Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  AAA support for dynamic Client based QoS and Security policies

- Per SSID bandwidth allocation

*** NOT available on CT 5760 at FCS
Marking at SSID is done via Mutation (table-map)

APs have several radios (2) – Each radio is shaped
Approximate Fair Drop and Wireless Queuing

Client VQ

SSID VQ

Radio VQ

Min or Max BW Allocation

Default Shaper

Radio Agg

Default Shaper

Data Queue

AFD BLOCK

Voice Queue

Video Queue

Weighted Scheduling

Strict Priority

Fair Bandwidth Allocation Courtesy of AFD – Without Configuration

Into a wired port

Out of a wireless port
The Catalyst 3850 QoS Toolbox

Wireless to Wired

Egress Wired Port

Priority Queue 1
Priority Queue 2
Queue
Queue
Queue

WTD

Marker
Policer
Marker
Policer
Marker
Policer

Classify

SSID Level

Marker
Policer
Marker
Policer
Marker
Policer

Client Level

Marker
Policer
Marker
Policer
Marker
Policer

Traffic

Out of a wired port
Into a wireless port
Agenda

- Catalyst 3850 – Overview
- Catalyst 3850 – Platform Architecture
- Catalyst 3850 – Stacking Architecture
- Catalyst 3850 – High Availability
- Catalyst 3850 – QoS
- Catalyst 3850 – Flexible NetFlow
- Catalyst 3850 – Key Takeaways
Typical NetFlow Deployment

NetFlow for Core Traffic Matrix
- Source/destination AS
- IP addresses (src/dest)
- BGP next hop
- Protocols
- DSCP

Server Flow Monitor
- Standard seven keys

Security Flow Monitor
- Protocol
- Ports
- IP addresses
- TCP flags

Managed Service Application Visibility
- IP addresses
- Application
- DSCP

Peering Flow Monitor
- Destination AS
- Source traffic index
- BGP next hop
- DSCP

ISP
Flexible NetFlow
Multiple Monitors with Unique Key Fields

Key Fields
- Source IP
- Destination IP
- Source Port
- Destination Port
- Layer 3 Protocol
- TOS Byte
- Input Interface

Non-Key Fields
- Packet 1
- Source IP
- Destination IP
- Source Port
- Destination Port
- Layer 3 Protocol
- TOS Byte
- Input Interface

Traffic Analysis Cache

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Source Port</th>
<th>Dest. Port</th>
<th>Protocol</th>
<th>TOS</th>
<th>Input I/F</th>
<th>...</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>2.2.2.2</td>
<td>23</td>
<td>22078</td>
<td>6</td>
<td>0</td>
<td>E0</td>
<td></td>
<td>1100</td>
</tr>
</tbody>
</table>

Security Analysis Cache

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Input I/F</th>
<th>Flag</th>
<th>...</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>2.2.2.2</td>
<td>E0</td>
<td>0</td>
<td></td>
<td>1100</td>
</tr>
</tbody>
</table>

• Top N talkers
• MAC, interface, VLAN
• 80+ Key Fields
• 14 Non-Key fields
Flexible Flow Record: Key Fields

<table>
<thead>
<tr>
<th>Flow</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampler ID</td>
<td>IP (Source or Destination)</td>
<td>IP (Source or Destination)</td>
</tr>
<tr>
<td>Direction</td>
<td>Payload Size</td>
<td>Payload Size</td>
</tr>
<tr>
<td>Class ID</td>
<td>Prefix (Source or Destination)</td>
<td>Prefix (Source or Destination)</td>
</tr>
<tr>
<td>Interface</td>
<td>Packet Section (Header)</td>
<td>Packet Section (Header)</td>
</tr>
<tr>
<td>Input</td>
<td>Mask (Source or Destination)</td>
<td>Mask (Source or Destination)</td>
</tr>
<tr>
<td>Output</td>
<td>Packet Section (Payload)</td>
<td>Packet Section (Payload)</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Minimum-Mask (Source or Destination)</td>
<td>Minimum-Mask (Source or Destination)</td>
</tr>
<tr>
<td>Source VLAN</td>
<td>TTL</td>
<td>DSCP</td>
</tr>
<tr>
<td>Dest VLAN</td>
<td>Options bitmap</td>
<td>Protocol</td>
</tr>
<tr>
<td>Dot1q VLAN</td>
<td>Version</td>
<td>Extension Headers</td>
</tr>
<tr>
<td>Dot1q priority</td>
<td>Precedence</td>
<td>Hop-Limit</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>Identification</td>
<td>Flow Label</td>
</tr>
<tr>
<td>Destination MAC address</td>
<td>DSCP</td>
<td>Length</td>
</tr>
</tbody>
</table>

NEW

NEW

© 2013 Cisco and/or its affiliates. All rights reserved. Cisco Public
### Flexible Flow Record: Key Fields

**Routing**
- src or dest AS
- Peer AS
- Traffic Index
- Forwarding Status
- IGP Next Hop
- BGP Next Hop

**Transport**
- Destination Port
- Source Port
- ICMP Code
- ICMP Type
- IGMP Type*
- TCP ACK Number
- TCP Header Length
- TCP Sequence Number
- TCP Window-Size
- TCP Source Port
- TCP Destination Port
- TCP Urgent Pointer

**Application**
- Application ID

**Multicast**
- Replication Factor*
- RPF Check Drop*
- Is-Multicast

**NEW: 2 or 4 bytes**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src or dest AS</td>
<td>Source or destination AS</td>
</tr>
<tr>
<td>Peer AS</td>
<td>Peer Autonomous System number</td>
</tr>
<tr>
<td>Traffic Index</td>
<td>Traffic Index</td>
</tr>
<tr>
<td>Forwarding Status</td>
<td>Forwarding Status</td>
</tr>
<tr>
<td>IGP Next Hop</td>
<td>IGP Next Hop</td>
</tr>
<tr>
<td>BGP Next Hop</td>
<td>BGP Next Hop</td>
</tr>
<tr>
<td>Input VRF Name</td>
<td>Input VRF Name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Port</td>
<td>Destination Port</td>
</tr>
<tr>
<td>Source Port</td>
<td>Source Port</td>
</tr>
<tr>
<td>ICMP Code</td>
<td>ICMP Code</td>
</tr>
<tr>
<td>ICMP Type</td>
<td>ICMP Type</td>
</tr>
<tr>
<td>IGMP Type*</td>
<td>IGMP Type*</td>
</tr>
<tr>
<td>TCP ACK Number</td>
<td>TCP Acknowledgment Number</td>
</tr>
<tr>
<td>TCP Header Length</td>
<td>TCP Header Length</td>
</tr>
<tr>
<td>TCP Sequence Number</td>
<td>TCP Sequence Number</td>
</tr>
<tr>
<td>TCP Window-Size</td>
<td>TCP Window-Size</td>
</tr>
<tr>
<td>TCP Source Port</td>
<td>TCP Source Port</td>
</tr>
<tr>
<td>TCP Destination Port</td>
<td>TCP Destination Port</td>
</tr>
<tr>
<td>TCP Urgent Pointer</td>
<td>TCP Urgent Pointer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Flag: ACK</td>
<td>TCP Acknowledgment Flag: ACK</td>
</tr>
<tr>
<td>TCP Flag: CWR</td>
<td>TCP Congestion Window Reset Flag: CWR</td>
</tr>
<tr>
<td>TCP Flag: ECE</td>
<td>TCP Extension Code: ECE</td>
</tr>
<tr>
<td>TCP Flag: FIN</td>
<td>TCP Finish</td>
</tr>
<tr>
<td>TCP Flag: PSH</td>
<td>TCP Push</td>
</tr>
<tr>
<td>TCP Flag: RST</td>
<td>TCP Reset</td>
</tr>
<tr>
<td>TCP Flag: SYN</td>
<td>TCP Synthesis</td>
</tr>
<tr>
<td>TCP Flag: URG</td>
<td>TCP Urgent Pointer</td>
</tr>
<tr>
<td>UDP Message Length</td>
<td>UDP Message Length</td>
</tr>
<tr>
<td>UDP Source Port</td>
<td>UDP Source Port</td>
</tr>
<tr>
<td>UDP Destination Port</td>
<td>UDP Destination Port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP SSRC</td>
<td>RTP Source Specific Receive Sequence Number</td>
</tr>
</tbody>
</table>

*IPv4 Flow only

**NEW**
### Flexible Flow Record: Non-Key Fields

<table>
<thead>
<tr>
<th>Counters</th>
<th>Timestamp</th>
<th>IPv4</th>
<th>IPv4 and IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>sysUpTime First Packet</td>
<td>Total Length Minimum (*)</td>
<td>Total Length Minimum (**)</td>
</tr>
<tr>
<td>Bytes Long</td>
<td>sysUpTime First Packet</td>
<td>Total Length Maximum (*)</td>
<td>Total Length Maximum (**)</td>
</tr>
<tr>
<td>Bytes Square Sum</td>
<td>Absolute first packet</td>
<td>TTL Minimum</td>
<td>TTL Maximum</td>
</tr>
<tr>
<td>Bytes Square Sum Long</td>
<td>Absolute last packet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packets Long</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bytes replicated</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bytes replicated Long</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packets replicated</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packets Replicated Long</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Plus any of the potential “key” fields: will be the value from the first packet in the flow

(*) IPV4_TOTAL_LEN_MIN, IPV4_TOTAL_LEN_MAX
(**)IP_LENGTH_TOTAL_MIN, IP_LENGTH_TOTAL_MAX
Three Types of NetFlow Caches

- Normal cache (traditional NetFlow)
  - More flexible active and inactive timers: one second minimum

- Immediate cache
  - Flow accounts for a single packet
  - Desirable for real-time traffic monitoring, DDoS detection, logging
  - Desirable when only very small flows are expected (e.g., sampling)
  - Caution: may result in a large amount of export data

- Permanent cache
  - To track a set of flows without expiring the flows from the cache
  - Entire cache is periodically exported (update timer)
  - After the cache is full (size configurable), new flows will not be monitored
  - Uses update counters rather than delta counters
Flexible NetFlow Top Talkers: Example

- The top 100 pairs of IP addresses with one or two packet(s) that are destined for “My Servers Network”

Router# show flow monitor <monitor> cache
  filter ipv4 destination address 10.10.10.0/24
  counter packet regex[1-2]
  aggregate ipv4 source address
    ipv4 destination address
  sort highest flow top 100
Embedded Event Manager 3.0
Flexible NetFlow Event Detector

flow record <my-record>
   match ipv4 ttl
   match ipv4 source address
   match ipv4 destination address

flow exporter <my-exporter>
   destination 10.10.10.10

flow monitor <my-monitor>
   record <my-record>
   exporter <my-exporter>

event manager applet security-applet
   event nf monitor-name "<my-monitor>" event-type create event1
   entry-value "5" field ipv4 ttl entry-op lt
   action 1.0 syslog msg "flow record with low TTL"

- If a flow record is created with TTL < 5, send a syslog message
Flexible NetFlow on Catalyst 3850

- **System Scalability**: Up to 19K per ASIC (with 80% utilization efficiency) cached flows for Forwarding Engine (24K Raw)
- **Bridged NetFlow**: Capability of creating and tracking bridged flows
- **TCP Flags**: are now exported as part of the flow information.
- **Export version 9**: (the most flexible)
- Ingress and Egress NetFlow support
- NetFlow sampling support (1 in 2-1024)
- Individual Stack member exports its own NetFlow records to Collector
- **Microflow policing**: supported for **Wireless** clients only at FCS
- Per-port, Per-Vlan
- Dynamic top talker support
- Supports 16 flow masks and 3 for Wireless Microflow QoS
- IPv6 NetFlow support
Agenda

Catalyst 3850 – Overview
Catalyst 3850 – Platform Architecture
Catalyst 3850 – Stacking Architecture
Catalyst 3850 – High Availability
Catalyst 3850 – QoS
Catalyst 3850 – Flexible NetFlow

Catalyst 3850 – Key Takeaways
Catalyst 3850 –
Key Takeaways

- UADP ASIC
  - Flex Parser, Lookups and Rewrites
  - Linderate Netflow 24K Flows
  - Converged Wired & Wireless

- 480 G of Stack BW
- 8 Queues/Port shaping & Scheduling
- 56 GE/ASIC @ 64 bytes

- Hosted Applications
  - (WCM, Wireshark*)
- Modular Design
- Converged Release*

- IOS-XE
  - Based on IOS/1+1 SSO Infra

- Stack-Wise-480 & HA
- Efficient Multicast Replication
- Distributed Forwarding

- Redundant Centralized CP

- SSO/NFS + AP SSO

© 2013 Cisco and/or its affiliates. All rights reserved. Cisco Public
Monitorování provozu datových sítí
Využití Cisco NetFlow v praxi

INVEA-TECH a.s.
info@invea.cz
Technologie NetFlow

- SNMP – pouze objemové ukazatele ze síťových rozhraní
- NetFlow – podrobné statistiky o provozu datové sítě
  - Cisco standard
  - Dostupné ve směrovačích a přepínačích
  - Kdo s kým, kolik, jak dlouhou
  - Next generation monitoring
Provozní i bezpečnostní využití

- Struktura a charakter provozu
- Identifikace provozních problémů a jejich příčin
- Odhalování infikovaných stanic, útoků a pokročilých hrozeb
- Odhalování nežádoucích aplikací
Struktura a charakter provozu

- 10% uživatelů typicky vygeneruje 90% provozu – kteří to jsou?
- Jak jsou využívány služby a proč byla včera síť tak pomalá?
Provozní problémy a příčiny

- Chybné konfigurace a výpadky služeb
DNSChanger: FBI Warns Infected Computers Will Lose Web, Email Access in July

Summary

DNSChanger is a trojan that will change the infected system's Domain Name System (DNS) traffic to unsolicited, and potentially illegal, sites.

The trojan is usually a small file (about 1.5 kilobytes) that is designed to change a computer's custom IP address. This IP address is usually encrypted in the body of a trojan package that a hacker will download. When a trojan-infected computer will contact the newly assigned DNS server to resolve names of different websites.
Worm spreads via Windows Remote Desktop

Anti-virus software vendor F-Secure is warning of a piece of malware by the name of Morto, which spreads using Windows' Remote Desktop Server (RDP server). It does not exploit a Windows security vulnerability. Instead, it scans IP address ranges for RDP port 3389 and then tries to log in as an administrator to any computers which respond using a list of common passwords.

**Event details**

- **Type:** RDP Dictionary Attacks (RDPDICTION)
- **Timestamp:** 2013-01-25 10:10:10
- **Event source:** 202.105.183.89
- **Event source host:** N/A
- **NetFlow source:** localhost
- **Probability:** 100 %
- **False positive:** No
- **Detail:** Continuation of attack, total count of targets: 1, current maximal transfer: 4.32 KiB, current count of attempts: 17. Part of distributed attack.
Malware from Peru Reportedly was sending AutoCAD Drawings to China

by SUNITHBABU (ONLINE) on JUNE 26, 2012
Nežádoucí aplikace

- **The Onion Router**
  - Klient pro různé OS
  - Nevýžaduje zvláštní schopnosti
  - Není možné detekovat analýzou obsahu
  - Vhodné pro obcházení politik a omezení

---

**Event details**

Type: The Onion Router (TOR)
Timestamp: 2012-05-09 13:06:59
Event source: 10.0.1.25
Event source host name: N/A
NetFlow source: localhost
Probability: 75%
False positive: No
Detail: Tor communication, unique onion routers: 51
Podpora konceptu BYOD

- Monitorování aktivních zařízení v síti
- Sledování přiřazení IP adresa – MAC adresa
  - Zpracování a analýza NetFlow z přístupové vrstvy
- Identifikace výrobce zařízení

<table>
<thead>
<tr>
<th>First Seen</th>
<th>Last Seen</th>
<th>IP address</th>
<th>MAC address</th>
<th>VLAN</th>
<th>Source</th>
</tr>
</thead>
</table>

Unique IP: 7
Unique MAC: 7
Total: 7
Řešení FlowMon

- **FlowMon Kolektor**
  - sběr a vizualizace síťových statistik
  - dlouhodobé uložení a reporting

- **FlowMon ADS**
  - detekce bezpečnostních a provozních událostí a anomálií
  - SW součást výbavy kolektoru
Nasazení řešení

• Centralizovaná architektura
  - Sběr NetFlow z jednoho nebo několika core přepínačů
  - Ukládání a vyhodnocování na centrálním kolektoru

• Sledovaný provoz
  - Klienti – WAN
  - Klienti – servery
  - Servery – WAN

• Vhodné pro
  - Datová centra
  - Velké podniky
Nasazení řešení

• Decentralizovaná architektura
  - Sběr NetFlow z řady hraničních routerů
  - Ukládání a vyhodnocování na centrálním kolektoru

• Sledovaný provoz
  - Lokalita – WAN
  - Lokalita – MPLS
  - Lokalita – DC

• Vhodné pro
  - Pobočky
Česká společnost, univerzitní spin-off, spolupráce CESNET a univerzity, projekty EU
Cisco Registered Developer
Založena 2007
Stovky instalací
Oblasti působení:
- Flow Monitoring
- Network Behavior Analysis

Zastavte se v předsálí a seznamte se s technologií FlowMon osobně a na živo
Děkuji za pozornost

Váš partner ve světě vysokorychlostních sítí

INVEA-TECH a.s.
info@invea.cz
511 205 250

INVEA-TECH a.s.
U Vodárny 2965/2
616 00 Brno
www.invea.cz
Otázky a odpovědi

Zodpovíme též v “Ptali jste se” v séle LEO v 17:45 – 18:30

e-mail: connect-cz@cisco.com
Prosíme, ohodnoťte tuto přednášku.
Děkujeme za pozornost.