ADDENDUM NO. 2 TO MASTER CO-BRANDED TECHNOLOGY SOLUTIONS AGREEMENT

This Addendum ("Addendum") to the Master Co-Branded Technology Solutions Agreement, executed concurrently ("Agreement") is entered into and is effective as of the date of last signature below (the "Addendum Effective Date"), by and between the Cisco entity defined in the Agreement ("Cisco"), and [redacted]. ("[redacted]"). All capitalized terms used but not otherwise defined in this Addendum have the meanings set forth in the Agreement.

This Addendum consists of this signature page and the following attachments, which are incorporated in this Addendum by this reference:
1. EXHIBIT A: Product Pricing& Productivity
2. EXHIBIT B: Unique Features
3. EXHIBIT C: System Functional Specification
4. EXHIBIT D: Switch Products
5. EXHIBIT E: Statement of Work
6. EXHIBIT F: Jointly Developed Technology

WHEREAS, Cisco and [redacted] have previously entered into the Agreement in order to set forth the general terms and conditions pursuant to which [redacted] may develop co-branded technology solutions in collaboration with Cisco and purchase and/or license Cisco Services and Products;

WHEREAS, the terms and conditions of the Agreement shall supersede all other agreements and addenda except insofar as there is a conflict in terms, in which case, the terms herein shall govern with respect to the [redacted] 7000; and

WHEREAS, Cisco and [redacted] wish to set forth the specific terms and conditions under which they shall collaborate to develop the [redacted] 7000 product for resale to resellers and End Users;

NOW THEREFORE, in consideration of the foregoing and the mutual promises and covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereto agree as follows:

1. **Definitions.** As used in this Addendum:

1.1. “AFC” or “Available For Customer” shall be defined as the time at which the Product has been accepted and approved by [redacted] for shipment to [redacted] customers as defined in the attached Statement of Work.
1.2. “Execution Commit” shall mean approval by Ethernet Switching Technology Group management of the specifications, schedule and budget for the Product development.
1.3. “Product” means, individually or collectively, as appropriate, one or more co-branded [redacted] 7000 products listed on Exhibit D, including both Hardware and Software as such exhibit may be amended from to time to time by written agreement of the Parties.

2. **Scope**.

2.1. Cisco will lead the development of the Product as stated in the Statement of Work attached hereto as Exhibit E. Cisco shall use best efforts to achieve the product development milestones set forth in the attached Statement of Work which includes but not limited to the following major Product development milestones as set forth below:

2.1.1. Cisco to provide [redacted] with working Prototypes as defined in the Statement of Work attached hereto as Exhibit E by August 31, 2011.

2.1.2. The commercial launch of the Product will be at the [redacted] in [redacted] (March 25, 2010).

2.1.3. The Product will be delivered to [redacted] for Acceptance Testing as defined in the Statement of Work to commence by [redacted] (May 2010).

3. **Term and Termination.**

3.1. This Addendum shall commence on the Addendum Effective Date and continue thereafter for a period of three (3) years, unless extended by written agreement of both parties or sooner terminated as set forth below. Without prejudice to either party's right to terminate this Addendum as set forth in sub-sections 12.2 to 12.5 of the Agreement, the agreement will be extended for two (2) two-year periods unless either party shall have given notice to the other party of it's intent not to extend the agreement at least twelve (12) months prior to the then-current expiration date. Any extension shall be on the same terms and conditions then in force, except as may be mutually agreed in writing by the parties. Notwithstanding the parties' right to extend the term of this Addendum, each party acknowledges that this Addendum shall always be interpreted as being limited in duration to a definite term and that the other party has made no commitments whatsoever regarding the duration or renewal of this Addendum beyond those expressly stated herein. The Parties agree that if [redacted] places Purchase Orders after the expiration of this Addendum, and Cisco accepts such Purchase Orders, then any such Purchase Orders shall be governed by the terms and conditions of this Addendum; provided, however that the placing of any Purchase Order by [redacted] or acceptance by Cisco of any Purchase Order placed after the Addendum has expired will not be considered as an extension of the term of the Addendum nor a renewal thereof. In any event, the terms and conditions of the Agreement shall survive termination with respect to this Addendum unless or until the Addendum has expired or been terminated in accordance with the terms incorporated herein.

3.2. Termination of this Addendum shall be in accordance with Section 12 of the Agreement.

4. [redacted] **Investment.** [redacted] will make a US $[redacted](4) Million ($[redacted](4,000,000.00) Non-Recurring Expense ("NRE") payment for the development of the Product as follows:

4.1. [redacted] will pay US $[redacted](2) Million ($[redacted]2,000,000.00) to Cisco upon execution of this Addendum and Cisco's Execute Commit approval for this Product.

4.2. [redacted] will pay the remaining US $[redacted](2) Million ($[redacted]2,00,000.00) as follows:

4.2.1. Milestone Payment #1: US $[redacted](800) Thousand ($[redacted]800,000) upon Cisco providing [redacted] with [redacted] approved working P2 Prototypes as defined in the Statement of Work attached here to as Exhibit E.
4.2.2. Milestone Payment #2: US $[redacted](800) Thousand ($[redacted]800,000) when the [redacted] 7000 is Available For Customers as defined in the Statement of Work attached here to as Exhibit E "Milestone #2 Commitment Date".

4.3. If Cisco cancels the Product development or if [redacted] determines the Product does not meet the Product acceptance terms set forth in the attached Statement of Work and cancels such Statement of Work, then Cisco shall refund all investment funds to [redacted] within thirty (30) days of notice of cancellation by either party.

4.4. If Cisco and [redacted] mutually agree that the Product has not substantially met the Systems Functional Specification requirements, attached hereto as Exhibit C, both parties agree to determine in good faith the appropriate time period for which Pricing Exhibit A-1 shall be in effect.

4.5. If Cisco elects not to renew this Addendum, terminate for convenience or obsolete the Product while the Pricing Schedule A-1 is in effect and [redacted] has not booked fifty-thousand (50,000) Products, then Cisco shall refund an amount to [redacted] within thirty days of [redacted] written request based on the following calculation: (50,000 – total unit bookings to date) X USD $40.00.

5. **Exclusivity.**

5.1. Cisco will provide [redacted] a six (6) month Product exclusivity period commencing on the Product AFC date. Cisco shall not authorize a third party to sell or publicly announce a partnership for the sale of a materially equivalent competing switch product (except for Cisco-only branded competing switch products).After the six (6) month Product exclusivity period, if Cisco authorizes a third party to sell or publicly announces a partnership for the sale of a materially equivalent competing switch product (except for Cisco-only branded competing switch products), Cisco shall extend to [redacted] no less favorable pricing for such products than Cisco extends to any other similarly situated private brand label or co-branded Product Partners.
5.2. In return, [redacted] agrees to not work with any new 3rd party switch vendor and introduce a materially equivalent competing switch product for that same six (6) month exclusivity period. [redacted] reserves the right to release a switch product to meet certain market requirements which are not covered by the current Product e.g. IP67 environmental specifications. [redacted] in good faith will provide Cisco with the first right of refusal for such product.

6. **Pricing.**

6.1. Prices for Products and Services shall be those specified in the Pricing Exhibit, attached hereto as Exhibit A-1 and A-2. Prices reflect the delivery terms stated in Section 5.0 of the Agreement.
6.2. The Product pricing terms shall be in accordance with this Addendum and the pricing Sections 3.3 through Section 3.7 of the Agreement.
6.3. Pricing Schedule A-1 is in effect for the first twenty-seven (27) months from AFC.
6.3.1. If Cisco makes a product similar to the Product available to any other party on a private brand label or co-branded basis after the six (6) month exclusivity

period but before end of the 12th month after the AFC date, Cisco will extend the Pricing Exhibit A-1 period of time from 27 to 33 months.

6.3.2. If Cisco makes a product similar to the Product available to any other party on a private brand label or co-branded basis between the 13th and 24th month after the AFC date, Cisco will extend the Pricing Exhibit A-1 period of time from 27 to 30 months.
6.3.3. If the three (3) or six (6) month extension period is required, Pricing Exhibit A-1 will remain in effect until [redacted] has booked 50,000 switches.
6.3.4. As soon as Pricing Exhibit A-1 has expired (including the expiration of any potential extension periods), Pricing Exhibit A-2 shall govern pricing.

7. **Productivity Improvement.** Cisco and [redacted] shall implement a productivity improvement plan after the first twenty-seven (27) months of AFC for the Product, the detailed requirements of which are set forth in the Pricing Exhibit attached hereto as Exhibit A.

8. **Unique Features.** The Product may contain unique features as defined further in Exhibit B ("Unique Features"). Such Unique Features will be made available only on the [redacted] Products. The parties agree to work in good faith to add new features that are deemed acceptable by both parties.

9. **Marketing.** [redacted] agrees to treat the announcement of the Products to the market as a major product launch by [redacted].

10. **Product Labeling.**
10.1 Cisco will label the [redacted] 7000product with the [redacted] name and switch product name based on [redacted] branding and logo standards set forth in [redacted] Publication 5910-7.0 guide dated January 2007. A Cisco ingredient brand will be applied to the product in accordance with Cisco branding and logo standards as referenced in the Agreement.
10.2 Front Panel Label: [redacted] and Cisco will use a common die cut shape, material callout, and adhesive for their respective labels. The color and artwork for each label will be different for [redacted] and Cisco. [redacted] is responsible for providing their label artwork to Cisco in a timely manner.
10.3 Compliance Label: There shall be one outline for all [redacted] SKUs and one outline for all Cisco SKUs. Label material and adhesive will be the same for [redacted] and Cisco. Artwork and content on each label may be configured differently for [redacted] and Cisco labels.
10.4 Cisco will create one Product ID for each [redacted] 7000 product, to include the product, documentation, and applicable packaging. The labels may contain the following information: Product description, Product number and series (Catalog number), System Level Part number and revision, catalog number bar code, WIN (warranty bar code), CIP serial number, MAC ID address, firmware revision, backplane requirements, country of origin, manufacturing date, TempMax for CSA, temperature code, and multiple rating symbols for agency markings.

10.5 Individual and bulk packaging for shipping will be designed in accordance with Cisco's standard packaging procedures with consideration given to [redacted] drawing number 95782800-A01, which includes packaging and palletization requirements and with changes to which both parties have agreed. The number of units per bulk or flow container will be defined by both parties at a later date. Both parties will review and approve final packaging, which will be documented in [redacted] Trading Goods Document (TGD).

10.6 A standard Cisco and [redacted] pack-out label will be used that will contain the Cisco Product ID. The serial number(s) of the product(s) in the box will be included on the label outside of the box in both human readable and bar coded formats. The country of origin will be identified on the outside labeling, as well.

10.7 No identifications with Cisco's name or logo will appear on any individual carton of the Switch Product shipped to [redacted] under this Agreement. A Cisco pack-out label and packing slip will accompany each order in the over-pack materials.

10.8 Cisco agrees to indicate the Hardware revision on each [redacted] switch. Layout of the labels will be done in accordance with a process to be agreed upon by both parties prior to Cisco's pre-pilot build.

10.9 The items identified above in this Section 10 are agreed to with respect to the switches and spares identified in Section A and B of Exhibit D. For new SFPs identified in Section C of Exhibit D, the current labeling, packaging requirements and process already established for existing SFPs will be followed.

11. **Confidentiality.** The obligations of each party with respect to Confidential Information disclosed under this Addendum are stated in Exhibit I of the Agreement, Supplement to Master Non-Disclosure Agreement Between Cisco Systems, Inc. and [redacted] Automation, (hereafter "NDA No. 115819"). In addition, Cisco shall retain as confidential all information associated with the Smartport and global macro configurations (i.e. macros) listed in Section 2 of Exhibit B (Stratix 7000 Unique Features or Modification), and Section 6.2 of NDA No.115819 shall not apply to terminate Cisco's confidentiality obligations with respect to the global macro and Smartport configurations.

12. **Survival.** Sections 1, 5, 8 and 11 and Exhibit B shall survive the expiration or termination of this Addendum.

IN WITNESS WHEREOF, the parties have caused this Addendum to be duly executed. Each party represents and warrants that its respective signatories, whose signatures appear below, are, on the date of signature, authorized to execute this Addendum.

Cisco [redacted]	[redacted]
By:	By:
James Doe	John Doe
Name: James Doe	Name: James Doe
Title: Executive	Title: Executive
Date: 05/26/12	Date: 05/26/12

[redacted]

APPROVED BY LEGAL

Exhibit A-1
Product Pricing & Productivity

A. Switch Products:

[redacted] Catalog No.	Description	Product Price
1783-BMS06SL	[redacted] 7000 4+2 SFP port, Lite SW	$275.88
1783-BMS06SA	[redacted] 7000 4+2 SFP port, Base SW	$391.42
1783-BMS06TL	[redacted] 7000 4+2 port, Lite SW	$275.88
1783-BMS06TA	[redacted] 7000 4+2 port, Base SW	$391.42
1783-BMS06SGL	[redacted] 7000 4+2 SFP Gig port, Lite SW	$337.36
1783-BMS06SGA	[redacted] 7000 4+2 SFP Gig port, Base SW	$448.66
1783-BMS06TGL	[redacted] 7000 4+2 Gig port, Lite SW	$337.36
1783-BMS06TGA	[redacted] 7000 4+2 Gig port, Base SW	$448.66
1783-BMS10CL	[redacted] 7000 8+2 combo port, Lite SW	$400.96
1783-BMS10CA	[redacted] 7000 8+2 combo port, Base SW	$585.40
1783-BMS10CGL	[redacted] 7000 8+2 combo Gig port, Lite SW	$490.00
1783-BMS10CGA	[redacted] 7000 8+2 combo Gig port, Base SW	$643.70
1783-BMS10CGP	[redacted] 7000 8+2 combo Gig port, Base SW, 1588	$690.34
1783-BMS10CGN	[redacted] 7000 8+2 combo Gig port, Base SW, 1588, NAT	$850.40
1783-BMS20CL	[redacted] 7000 16+2 SFP+2 combo port, Lite SW	$662.78
1783-BMS20CA	[redacted] 7000 16+2 SFP+2 combo port, Base SW	$1,017.88
1783-BMS20CGL	[redacted] 7000 16+2 SFP+2 combo Gig port, Lite SW	$743.34
1783-BMS20CGP	[redacted] 7000 16+2 SFP+2 combo Gig port, Base SW, 1588	$1,106.92
1783-BMS20CGPK	[redacted] 7000 16+2 SFP+2 combo Gig port, Base SW, 1588, Conformal coating	$1,247.90

The prices above do not include the services pricing.

B. Hardware Options

SD Flash with IOS installed $50

C. New SFPs:

Cisco Catalog item (PID)	[redacted] Catalog No.	Product Price
GLC-FE-100FX	1783-SFP100FXC	$ 87.50
GLC-FE-100LX	1783-SFP100LXC	$140.00
GLC-FE-100EX (v-02 or later)	1783-SFP100EXC	$208.25
GLC-FE-100ZX	1783-SFP100ZXC	$418.25
GLC-SX-MMD	1783-SFP1GSXE	$175.00
GLC-LH-SMD	1783-SFP1GLHE	$348.25
GLC-EX-SMD	1783-SFP1GEXE	$383.25
GLC-ZX-SM-RGD	1783-SFP1GZX	$1,540.00

The chart above represents the new SFPs which will be added to the existing list of SFPs productized by [redacted].

SERVICES AVAILABILITY

Switch Product Code	[redacted] Catalog No.	[redacted] [redacted] Description	Term	Service Price
CON-ETSPB	1783-BMS06SL	[redacted] 7000 4+2 SFP port, Lite SW	3 yrs	$25.27
CON-ETSPB	1783-BMS06SA	[redacted] 7000 4+2 SFP port, Base SW	3 yrs	$34.51
CON-ETSPB	1783-BMS06TL	[redacted] 7000 4+2 port, Lite SW	3 yrs	$25.27
CON-ETSPB	1783-BMS06TA	[redacted] 7000 4+2 port, Base SW	3 yrs	$34.51
CON-ETSPB	1783-BMS06SGL	[redacted] 7000 $+2 SFP Gig port, Lite SW	3 yrs	$30.19
CON-ETSPB	1783-BMS06SGA	[redacted] 7000 $+2 SFP Gig port, Base SW	3 yrs	$39.09
CON-ETSPB	1783-BMS06TGL	[redacted] 7000 4+2 Gig port, Lite SW	3 yrs	$30.19
CON-ETSPB	1783-BMS06TGA	[redacted] 7000 4+2 Gig port, Base SW	3 yrs	$39.09
CON-ETSPB	1783-BMS10CL	[redacted] 7000 8+2 SFP port, Lite SW	3 yrs	$35.28
CON-ETSPB	1783-BMS10CA	[redacted] 7000 8+2 SFP port, Base SW	3 yrs	$50.03
CON-ETSPB	1783-BMS10CGL	[redacted] 7000 8+2 SFP Gig port, Lite SW	3 yrs	$42.40
CON-ETSPB	1783-BMS10CGA	[redacted] 7000 8+2 SFP Gig port, Base SW	3 yrs	$54.70
CON-ETSPB	1783-BMS10CGP	[redacted] 7000 8+2 SFP Gig port, Base SW, 1588	3 yrs	$58.43
CON-ETSPB	1783-BMS10CGN	[redacted] 7000 8+2 SFP Gig port, Base SW, 1588, NAT	3 yrs	$71.23
CON-ETSPB	1783-BMS20CL	[redacted] 7000 16+4 SFP port, Lite SW	3 yrs	$56.22
CON-ETSPB	1783-BMS20CA	[redacted] 7000 16+4 SFP port, Base SW	3 yrs	$84.63
CON-ETSPB	1783-BMS20CGL	[redacted] 7000 16+4 SFP Gig port, Lite SW	3 yrs	$62.67
CON-ETSPB	1783-BMS20CGP	[redacted] 7000 16+4 SFP Gig port, Base SW, 1588	3 yrs	$91.75
CON-ETSPB 1783-	BMS20CGPK	[redacted] 7000 16+4 SFP Gig port, Base SW, 1588, CC	3 yrs	$103.03

Product Failure Analysis Service

Description of Service	Per Product Unit Cost
Failure Analysis Service for Products out of warranty or not covered by an active service contract	USD $1,150.00

Delivery

Cisco will provide switch products with a lead time of fourteen (14) calendar days from acceptance of [redacted] Purchase Order(s) to ship-confirm from the Cisco direct fulfillment site pursuant to Section 5.1.1 of the Agreement.

Exhibit A-2
Product Pricing & Productivity

A. Switch Products:

[redacted] Catalog No.	Description	Product Price
1783-BMS06SL	[redacted] 7000 4+2 SFP port, Lite SW	$315.88
1783-BMS06SA	[redacted] 7000 4+2 SFP port, Base SW	$431.42
1783-BMS06TL	[redacted] 7000 4+2 port, Lite SW	$315.88
1783-BMS06TA	[redacted] 7000 4+2 port, Base SW	$431.42
1783-BMS06SGL	[redacted] 7000 4+2 SFP Gig port, Lite	SW $377.36
1783-BMS06SGA	[redacted] 7000 4+2 SFP Gig port, Base SW	$488.66
1783-BMS06TGL	[redacted] 7000 4+2 Gig port, Lite SW	$377.36
1783-BMS06TGA	[redacted] 7000 4+2 Gig port, Base SW	$488.66
1783-BMS10CL	[redacted] 7000 8+2 combo port, Lite SW	$440.96
1783-BMS10CA	[redacted] 7000 8+2 combo port, Base SW	$625.40
1783-BMS10CGL	[redacted] 7000 8+2 combo Gig port, Lite SW	$530.00
1783-BMS10CGA	[redacted] 7000 8+2 combo Gig port, Base SW	$683.70
1783-BMS10CGP	[redacted] 7000 8+2 combo Gig port, Base SW, 1588	$730.34
1783-BMS10CGN	[redacted] 7000 8+2 combo Gig port, Base SW, 1588, NAT	$890.40
1783-BMS20CL	[redacted] 7000 16+2 SFP+2 combo port, Lite SW	$702.78
1783-BMS20CA	[redacted] 7000 16+2 SFP+2 combo port, Base SW	$1,057.88
1783-BMS20CGL	[redacted] 7000 16+2 SFP+2 combo Gig port, Lite SW	$783.34
1783-BMS20CGP	[redacted] 7000 16+2 SFP+2 combo Gig port, Base SW, 1588	$1,146.92
1783-BMS20CGPK	[redacted] 7000 16+2 SFP+2 combo Gig port, Base SW, 1588, Conformal coating	$1,287.90

The prices above do not include the services pricing.

B. Hardware Options
SD Flash with IOS installed $50

C. New SFPs:

Cisco Catalog item (PID)	[redacted] Catalog No.	Product Price
GLC-FE-100FX	1783-SFP100FXC	$ 87.50
GLC-FE-100LX	1783-SFP100LXC	$140.00
GLC-FE-100EX (v-02 or later)	1783-SFP100EXC	$208.25
GLC-FE-100ZX	1783-SFP100ZXC	$418.25
GLC-SX-MMD	1783-SFP1GSXE	$175.00
GLC-LH-SMD	1783-SFP1GLHE	$348.25
GLC-EX-SMD	1783-SFP1GEXE	$383.25
GLC-ZX-SM-RGD	1783-SFP1GZX	$1,540.00

The chart above represents the new SFPs which will be added to the existing list of SFPs productized by [redacted] Automation.

SERVICES AVAILABILITY

Switch Product Code	[redacted] Catalog No.	[redacted] Automation Description	Term Service	Price
CON-ETSPB	1783-BMS06SL	[redacted] 7000 4+2 SFP port, Lite SW	3 yrs	$25.27
CON-ETSPB	1783-BMS06SA	[redacted] 7000 4+2 SFP port, Base SW	3 yrs	$34.51
CON-ETSPB	1783-BMS06TL	[redacted] 7000 4+2 port, Lite SW	3 yrs	$25.27
CON-ETSPB	1783-BMS06TA	[redacted] 7000 4+2 port, Base SW	3 yrs	$34.51
CON-ETSPB	1783-BMS06SGL	[redacted] 7000 $+2 SFP Gig port, Lite SW	3 yrs	$30.19
CON-ETSPB	1783-BMS06SGA	[redacted] 7000 $+2 SFP Gig port, Base SW	3 yrs	$39.09
CON-ETSPB	1783-BMS06TGL	[redacted] 7000 4+2 Gig port, Lite SW	3 yrs	$30.19
CON-ETSPB	1783-BMS06TGA	[redacted] 7000 4+2 Gig port, Base SW	3 yrs	$39.09
CON-ETSPB	1783-BMS10CL	[redacted] 7000 8+2 SFP port, Lite SW	3 yrs	$35.28
CON-ETSPB	1783-BMS10CA	[redacted] 7000 8+2 SFP port, Base SW	3 yrs	$50.03
CON-ETSPB	1783-BMS10CGL	[redacted] 7000 8+2 SFP Gig port, Lite SW	3 yrs	$42.40
CON-ETSPB	1783-BMS10CGA	[redacted] 7000 8+2 SFP Gig port, Base SW	3 yrs	$54.70
CON-ETSPB	1783-BMS10CGP	[redacted] 7000 8+2 SFP Gig port, Base SW, 1588	3 yrs	$58.43
CON-ETSPB	1783-BMS10CGN	[redacted] 7000 8+2 SFP Gig port, Base SW, 1588, NAT	3 yrs	$71.23
CON-ETSPB	1783-BMS20CL	[redacted] 7000 16+4 SFP port, Lite SW	3 yrs	$56.22
CON-ETSPB	1783-BMS20CA	[redacted] 7000 16+4 SFP port, Base SW	3 yrs	$84.63
CON-ETSPB	1783-BMS20CGL	[redacted] 7000 16+4 SFP Gig port, Lite SW	3 yrs	$62.67
CON-ETSPB	1783-BMS20CGP	[redacted] 7000 16+4 SFP Gig port, Base SW, 1588	3 yrs	$91.75
CON-ETSPB	1783-BMS20CGPK	[redacted] 7000 16+4 SFP Gig port, Base SW, 1588, CC	3 yrs	$103.03

D. PRODUCTIVITY

Transfer Price Reduction. If, [redacted] achieves 30,000 unit sales within its fiscal year ([redacted](June 1st) through [redacted](May 30th), Cisco will reduce the price per unit by [redacted](2)% in the following fiscal year. There will be an additional [redacted](3)% reduction in price per unit for each increment of 15,000 in sales in a fiscal year up to a maximum reduction in price per unit of [redacted](10)% for achieving 75,000 unit sales in a fiscal year.

Transfer price reduction shall go into effect during the fiscal year following the fiscal year in which [redacted] achieved the aforementioned increases in sales and shall remain in effect as long as [redacted] meets or exceeds the trigger condition. If [redacted] fails to meet the trigger condition in any fiscal year, the transfer price reduction is removed for the following year. Cisco is exempt from applying the transfer price reduction to the [redacted] 7000 product while Pricing Schedule A-1 is in effect.

The calculation of all pricing reductions described in this section D, shall be based off of the unit product pricing stated in the pricing schedule A-2 above.

Exhibit B
[redacted] 7000 Unique Features or Modifications

Section 1

The parties mutually agree that the following existing switch modifications and naming conventions shall be made available on the [redacted] Switch Product as specifically set forth below.

1. [redacted] 7000 Smartports for [redacted] markets as named below:

External Name	Internal Macro Name	Icons
Automation Devices	(ab-ethernetip)	
Multiport Automation Devices	(ab-multiport-device)	
Desktop for Automation	(desktop-automation)	
Virtual Desktop for Automation	(vm-desktop-automation)	
Switch for Automation	(switch-automation)	
Router for Automation	(router-automation)	
Phone for Automation	(phone-automation)	
Wireless for Automation	(wireless-automation)	
	(none-automation)	

Each Smartport will include three components; an icon, a name and a configuration. The parties agree that Cisco shall have the right to make, market, distribute and sell products to other partners and end users that contain Smartport configurations. Cisco shall not, however, use or provide to any third party names or icons identical to the Smartport icons and names listed above.

2. [redacted] version of Device Manager consisting of a [redacted] style look and feel based on the [redacted] Automation Embedded Web Style Guide and [redacted] online help. Details are defined in the [redacted] 8000 addendum System Functional Specification (Exhibit C, Appendix C). The content of the Device Manager is not unique to [redacted].

3. Switch configuration for [redacted] Switch Product when initial IP address is set, as defined by the global Smartport macros below:

ab-global
ab-qos-map-setup
ab-qos-queue-setup
ab-password

Preliminary details of these macros are defined below in Section 2 of this Exhibit and are subject to change as agreed to by both parties. The parties agree that Cisco shall have the right to make, market, distribute and sell product to other partners that contain Smartport configurations, but shall not use or provide to any third party the names of [redacted] versions of the ab-global, ab-qos-map-setup, ab-qos-queuesetup, and ab-password macros.

4. [redacted] specific values for vendor ID, CIP serial numbers, product code, and product name string attributes in the CIP Identity Object should be unique to the [redacted] 7000.Details to be mutually defined and agreed to by the parties in the [redacted] 7000 Functional Specification Exhibit C,Sections3.13, 4.3.1.1, 4.3.1.2, 4.3.1.4 and 4.3.1.5.
5. MAC (Media Access Control) addresses and product serial numbers from [redacted] Automation allocation should be unique to the [redacted] 7000.Reference the [redacted] 7000 Functional Specification Exhibit C, Sections 4.3.1.3, 4.3.1.5 and 3.13.

Section 2

ab-global

```
#macro keywords $cip_vlan
# Macro Name ab-global
#macro global description ab-global
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
no aaa new-model
service timestamps log datetime msec localtime showtimezone
service timestamps debug datetime msec localtime showtimezone
service password-encryption
logging buffered 16384 debugging
no logging console
vtp mode transparent
udld aggressive
no ip source-route
no ip domain-lookup
ip subnet-zero
ip igmp snooping
ip igmp snooping querier
errdisable recovery cause all
errdisable recovery interval 30
spanning-tree mode mst
spanning-tree loopguard default
spanning-tree portfast bpduguard default
spanning-tree portfast bpdufilter default
int vlan $cip_vlan
cip enable
exit
alarm profile ab-alarm
alarm 1 2 3 4
syslog 1 2 3 4
notifies 1 2 3 4
relay-major 2
relay-minor 1 3 4
exit
```

```
alarm facility power-supply relay major
alarm facility power-supply syslog
alarm facility power-supply notifies
alarm facility temperature primary relay major
alarm facility temperature primary syslog
alarm facility temperature primary notifies
alarm facility temperature secondary relay minor
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
alarm facility temperature secondary high 90
alarm facility temperature secondary low 0
snmp-server enable traps
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
class-map match-all CIP-Implicit_dscp_55
match access-group 101
class-map match-all CIP-Implicit_dscp_47
match access-group 102
class-map match-all CIP-Implicit_dscp_43
match access-group 103
class-map match-all CIP-Implicit_dscp_any
match access-group 104
class-map match-all CIP-Other
match access-group 105
class-map match-all 1588-PTP-Event
match access-group 106
class-map match-all 1588-PTP-General
match access-group 107
class-map match-all voip-data
match ip dscp ef
class-map match-all voip-control
match ip dscp cs3 af31
policy-map Voice-Map
class voip-data
set dscp ef
police 320000 8000 exceed-action policed-dscptransmit
class voip-control
set dscp cs3
police 32000 8000 exceed-action policed-dscptransmit
policy-map CIP-PTP-Traffic
class CIP-Implicit_dscp_55
set ip dscp 55
                      class CIP-Implicit_dscp_47
```

```
set ip dscp 47
class CIP-Implicit_dscp_43
set ip dscp 43
class CIP-Implicit_dscp_any
set ip dscp 31
class CIP-Other
set ip dscp 27
class 1588-PTP-Event
set ip dscp 59
class 1588-PTP-General
set ip dscp 47
```

ab-qos-map-setup

```
#macro name ab-qos-map-setup
mls qos map policed-dscp 24 27 31 43 46 47 55 59 to 0
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue input threshold 1 16 66
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 40 60
mls qos srr-queue input bandwidth 40 60
mls qos map dscp-cos 0 1 2 3 4 5 6 7 to 0
mls qos map dscp-cos 9 11 12 13 14 15 to 0
mls qos map dscp-cos 8 10 to 1
mls qos map dscp-cos 16 17 18 19 20 21 22 23 to 2
mls qos map dscp-cos 25 26 28 29 30 to 2
mls qos map dscp-cos 24 27 31 to 3
mls qos map dscp-cos 32 33 34 35 36 37 38 39 to 4
mls qos map dscp-cos 40 41 42 44 45 49 to 4
mls qos map dscp-cos 50 51 52 53 54 56 57 58 to 4
mls qos map dscp-cos 60 61 62 63 to 4
mls qos map dscp-cos 43 46 47 to 5
mls qos map dscp-cos 48 55 to 6
mls qos map dscp-cos 59 to 7
no mls qos rewrite ip dscp
# Return the egress queue-set configurations to
default
no mls qos queue-set output 1 threshold 2
no mls qos queue-set output 1 threshold 2
no mls qos queue-set output 1 threshold 3
no mls qos queue-set output 1 threshold 4
no mls qos queue-set output 2 threshold 1
no mls qos queue-set output 2 threshold 2
no mls qos queue-set output 2 threshold 3
no mls qos queue-set output 2 threshold 4
```

ab-qos-queue-setup

```
#macro name ab-qos-queue-setup
```

mls qos srr-queue input cos-map queue 1 threshold 2 1

mls qos srr-queue input cos-map queue 1 threshold 3 0 2
mls qos srr-queue input cos-map queue 2 threshold 2 4
mls qos srr-queue input cos-map queue 2 threshold 3 3 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 2 8 10
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 9 11 12 13 14 15 16
mls qos srr-queue input dscp-map queue 1 threshold 3 17 18 19 20 21 22 23 25
mls qos srr-queue input dscp-map queue 1 threshold 3 26 28 29 30
mls qos srr-queue input dscp-map queue 2 threshold 2 32 33 34 35 36 37 38 39
mls qos srr-queue input dscp-map queue 2 threshold 2 40 41 42 44 45 49 50 51
mls qos srr-queue input dscp-map queue 2 threshold 2 52 53 54 56 57 58 60 61
mls qos srr-queue input dscp-map queue 2 threshold 2 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 27 31 43 46 47 48 55
mls qos srr-queue input dscp-map queue 2 threshold 3 59
mls qos srr-queue output cos-map queue 1 threshold 3 7
mls qos srr-queue output cos-map queue 2 threshold 2 1
mls qos srr-queue output cos-map queue 2 threshold 3 0 2 4
mls qos srr-queue output cos-map queue 3 threshold 3 5 6
mls qos srr-queue output cos-map queue 4 threshold 3 3
mls qos srr-queue output dscp-map queue 1 threshold 3 59
mls qos srr-queue output dscp-map queue 2 threshold 2 8 10
mls qos srr-queue output dscp-map queue 2 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 2 threshold 3 9 11 12 13 14 15
mls qos srr-queue output dscp-map queue 2 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 3 25 26 28 29 30 32
mls qos srr-queue output dscp-map queue 2 threshold 3 33 34 35 36 37 38 39 40
mls qos srr-queue output dscp-map queue 2 threshold 3 41 42 44 45 49 50 51 52
mls qos srr-queue output dscp-map queue 2 threshold 3 53 54 56 57 58 60 61 62
mls qos srr-queue output dscp-map queue 2 threshold 3 63
mls qos srr-queue output dscp-map queue 3 threshold 3 43 46 47 48 55
mls qos srr-queue output dscp-map queue 4 threshold 3 24 27 31
mls qos queue-set output 1 buffers 10 25 40 25
mls qos queue-set output 2 buffers 10 25 40 25
mls qos,

ab-password

```
# macro keywords $password $RO-password
#macro name ab-password
enable secret $password
/* Enhancement as per Device manager requirements */
enable secret level 1 $RO-password
cip security password $password
line con 0
password $password
line vty 0 15
password $password
```

ab-ethernetip

```
# macro keywords $access_vlan
#macro description ab-ethernetip
switchport host
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport access vlan $access_vlan
service-policy input CIP-PTP-Traffic
priority-queue out
srr-queue bandwidth share 1 19 40 40
alarm profile ab-alarm
load-interval 30
no cdp enable
```

desktop-automation

```
#macro keywords $access_vlan
#macro name desktop-automation
switchport mode access
switchport access vlan $ACCESS_VLAN
switchport port-security
switchport port-security maximum 1
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input CIP-PTP-Traffic
no alarm profile
alarm profile ab-alarm
```

switch-automation

```
#macro keywords $native_vlan
#macro name: switch-automation
switchport mode trunk
switchport trunk native vlan $NATIVE_VLAN
spanning-tree link-type point-to-point
mls qos trust cos
service-policy input CIP-PTP-Traffic
priority-queue out
srr-queue bandwidth share 1 19 40 40
no alarm profile
alarm profile ab-alarm
```

router-automation

```
#macro keywords $native_vlan
#Macro name router-automation
switchport mode trunk
switchport trunk native vlan $NATIVE_VLAN
spanning-tree portfast trunk
spanning-tree bpduguard enable
mls qos trust dscp
service-policy input CIP-PTP-Traffic
priority-queue out
srr-queue bandwidth share 1 19 40 40
no alarm profile
alarm profile ab-alarm
```

phone-automation

```
#macro keywords: $access_vlan $voice_vlan
#macro name phone-automation
switchport mode access
switchport access vlan $ACCESS_VLAN
switchport voice vlan $VOICE_VLAN
switchport port-security
switchport port-security maximum 2
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
no service-policy input CIP-PTP-Traffic
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input Voice-Map
srr-queue bandwidth share 10 10 60 20
no alarm profile
alarm profile ab-alarm
```

wireless-automation

```
#macro keywords: $native_vlan
#macro name: wireless-automation
switchport mode trunk
switchport trunk native vlan $NATIVE_VLAN
switchport nonegotiate
spanning-tree bpduguard enable
mls qos trust cos
service-policy input CIP-PTP-Traffic
srr-queue bandwidth share 1 19 40 40
no alarm profile
                        alarm profile ab-alarm
```

ab-multiport-device

```
# macro keywords $access_vlan
#macro description ab-multiport-device
switchport host
switchport access vlan $access_vlan
service-policy input CIP-PTP-Traffic
priority-queue out
srr-queue bandwidth share 1 19 40 40
alarm profile ab-alarm
load-interval 30
no cdp enable
no udld port aggressive
mls qos trust dscp
```

vm-desktop-automation

```
#macro keywords $access_vlan
#macro name vm-desktop-automation
switchport mode access
switchport access vlan $ACCESS_VLAN
switchport port-security
switchport port-security maximum 2
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input CIP-PTP-Traffic
no alarm profile
alarm profile ab-alarm
```

none-automation

```
#macro keywords: -
#macro name: none-automation
alarm profile ab-alarm
no service-policy input Voice-Map
service-policy input CIP-PTP-Traffic
                        no macro description
```

Exhibit B-2

The following sets forth a list of additional features, which the parties by mutual agreement may deem to be Unique Features of the [redacted] Automation Switch Product. This list will be reviewed annually at the business reviews to update such list as acceptable by both parties.

1. (Not yet determined by the parties.)
2.
3.

The following features are merely recommendations by [redacted] as to features, which the parties may wish to add to the list of [redacted] Unique Features set forth in Exhibit A-2. Unless the parties expressly agree, the following features shall not be deemed to be Unique Features of the [redacted] Switch Product. However, the parties agree to work in good faith at the quarterly business reviews to determine whether and to what extent the following features may become Unique Features, as well as whether and to what extent any additional features may be added to Exhibit A-2 as additional Unique Features of the [redacted] Switch Product. The parties agree that after a feature is added to the list in Exhibit A-2, it be cannot be removed until both parties mutually agree to remove it. Examples of such features include but are not limited to the following:

1. Writing CIP parameters via CIP explicit messaging except as required to be compliant with ODVA EtherNet/IP specification. Reference TBD.
2. The up/down loading of switch configuration and other file objects via CIP messaging except for EDS. Reference TBD.
3. Read CIP parameters without a password. Reference TBD.
4. CIP exclusive owner I/O connection which provides for enabling/disabling of switch ports. Reference TBD.

Exhibit C – System Functional Specification
(To be attached as a separate document.)

EDCS-982269 through revision #71

Exhibit D – Switch Products

A. Switch Products:

Nineteen (19) catalog items for the Stratix 7000 family of switches as listed below:

[redacted] Catalog No.	Description
1783-BMS06SL	Stratix 7000 4+2 SFP port, Lite SW
1783-BMS06SA	Stratix 7000 4+2 SFP port, Base SW
1783-BMS06TL	Stratix 7000 4+2 port, Lite SW
1783-BMS06TA	Stratix 7000 4+2 port, Base SW
1783-BMS06SGL	Stratix 7000 4+2 SFP Gig port, Lite SW
1783-BMS06SGA	Stratix 7000 4+2 SFP Gig port, Base SW
1783-BMS06TGL	Stratix 7000 4+2 Gig port, Lite SW
1783-BMS06TGA	Stratix 7000 4+2 Gig port, Base SW
1783-BMS10CL	Stratix 7000 8+2 combo port, Lite SW
1783-BMS10CA	Stratix 7000 8+2 combo port, Base SW
1783-BMS10CGL	Stratix 7000 8+2 combo Gig port, Lite SW
1783-BMS10CGA	Stratix 7000 8+2 combo Gig port, Base SW
1783-BMS10CGP	Stratix 7000 8+2 combo Gig port, Base SW, 1588
1783-BMS10CGN	Stratix 7000 8+2 combo Gig port, Base SW, 1588, NAT
1783-BMS20CL	Stratix 7000 16+2 SFP+2 combo port, Lite SW
1783-BMS20CA	Stratix 7000 16+2 SFP+2 combo port, Base SW
1783-BMS20CGL	Stratix 7000 16+2 SFP+2 combo Gig port, Lite SW
1783-BMS20CGP	Stratix 7000 16+2 SFP+2 combo Gig port, Base SW, 1588
1783-BMS20CGPK	Stratix 7000 16+2 SFP+2 combo Gig port, Base SW, 1588, Conformal coating

Note: the Cisco Product ID will consist of the [redacted] Catalog number and series identifier.

B. Hardware Options

[redacted] Catalog No.	Description
1783-BMSD	SD flash card with IOS installed

Note: the Cisco Product ID will consist of the [redacted] Catalog number and series identifier.

C. SFPs:

The SFPs that will be supported on the Stratix 7000 switches. This includes new SFPs and existing SFPs.

Cisco Catalog item (PID)	[redacted] Catalog No.	Description
GLC-FE-100FX	1783-SFP100FXC	100BASE-FX SFP module for 100-MB ports, 1310 nm wavelength,
GLC-FE-100LX	1783-SFP100LXC	100BASE-LX SFP module for 100-MB ports, 1310 nm wavelength

GLC-FE-100EX (v-02 or later)	1783-SFP100EXC	100BASE-EX SFP module for 100-MB ports, 1310 nm wavelength
GLC-FE-100ZX	1783-SFP100ZXC	100BASE-ZX SFP module for 100-MB ports, 1550 nm wavelength
GLC-SX-MMD	1783-SFP1GSXE	1000BASE-SX SFP transceiver module for MMF,850-nm wavelength, extended operating temperaturerange and DOM support, dual LC/PC connector
GLC-LH-SMD	1783-SFP1GLHE	1000BASE-LX/LH SFP transceiver module for MMFand SMF, 1300-nm wavelength, extended operatingtemperature range and DOM support, dual LC/PCconnector
GLC-EX-SMD	1783-SFP1GEXE	1000BASE-EX SFP transceiver module for SMF,1310-nm wavelength, extended operating temperaturerange and DOM support, dual LC/PC connector
GLC-ZX-SM-RGD	1783-SFP1GZX	1000BASE-ZX SFP transceiver module for SMF,1550-nm wavelength, industrial Ethernet, dual LC/PCconnector
GLC-FE-100FX-RGD	1783-SFP100FX	100BASE-FX SFP module for Industrial Ethernet 100-MB ports, 1310 nm wavelength
GLC-FE-100LX-RGD	1783-SFP100LX	100BASE-LX SFP module for Industrial Ethernet 100-MB ports, 1310 nm wavelength
GLC-SX-MM-RGD	1783-SFP1GSX	1000BASE-SX SFP transceiver module for MMF,850-nm wavelength, industrial Ethernet, dual LC/PCconnector
GLC-LX-SM-RGD	1783-SFP1GLX	1000BASE-LX/LH SFP transceiver module for MMFand SMF, 1300-nm wavelength, industrial Ethernet,dual LC/PC connector

The first eight (8) above represent new SFPs, which will be added to the existing four (4) SFPs productized by [redacted] Automation.

Exhibit E
[redacted] 7000 - STATEMENT OF WORK
Cisco / [redacted] Automation Confidential

This exhibit is the Statement of Work under Addendum 2 of the Master Co-Branding Agreement by and between Cisco Systems, Inc. ("Cisco") and [redacted] Automation, Inc. ("[redacted]"). The exhibit describes the scope product development work to be performed by Cisco and [redacted] during development of the Product.

1.0 DEFINITIONS (As used in this Exhibit)

1.1 Product Validation Testing – Shall mean testing performed by Cisco during Product development to assure all defined features perform as expected over the specified range of operating conditions. Validation Testing includes Characterization as well as Functional, Mechanical, Thermal and Software Feature, System and Regression Testing.

1.2 System Integration Testing – Shall mean acceptance testing performed by [redacted] under conditions that emulate the user's application and environmental conditions.

1.3 Acceptance Testing – Shall mean System Integration and additional compliance testing performed by [redacted] on Pre-Pilot units to determine if the Product conforms to specifications and is ready for AFC release.

1.4 CIP Enhancements – shall mean new CIP features that do not exist on the current [redacted] 8000

2.0 [redacted] PRODUCT

· [redacted] Automation [redacted] 7000 is a [redacted] Automation Industrial Ethernet switch product family, designed and manufactured by Cisco. All of the switch products are considered to be networking infrastructure equipment. Details of the features to be provided are provided in the [redacted] 7000 System Functional Specification (SFS), attached as Exhibit C to Addendum 2 of the Master Agreement.

· [redacted] and Cisco shall work together to define a Product Validation and System Integration Test strategy. Cisco is responsible for the definition, execution and documentation of the Product Validation Tests and associated results. [redacted] is responsible for the definition, execution and documentation of the System Integration Tests and associated results. [redacted] will review and provide feedback on both the tests plans and results. [redacted] will conduct an acceptance test of the [redacted] 7000 product prior to AFC release.

3.0 PROGRAM MANAGERS

The following individuals shall be the Program Managers for the work performed in this Statement of Work:

Homer Hegedus	Larry Martis
Cisco Systems, Inc.	[redacted] Automation, Inc.
12515 Research Blvd., Bldg.4	[redacted]

Austin, TX 78759	City, State
Phone: 512-378-2905	Phone Number
Email: hhegedus@cisco.com	Email

4.0 PROTOTYPES

Cisco will deliver to [redacted] the quantity of the prototypes shown in the table below at no additional charge.
Note: each line represents a single HW configuration capable of multiple SW configurations

Group	Stratix 7000 Catalog Number	P1B Qty	P2 Qty	PP Qty
1	1783-BMS06TGA	2	2	2
1	1783-BMS06SGA	2	2	2
1	1783-BMS10CGA	2	2	2
2	1783-BMS10CGN	3	8	2
2	1783-BMS20CGP	3	2	2
2	1783-BMS20CGPK	0	0	2

Key:
4/8/16 = number of downlinks
G = Gigabit Uplinks
S = SFP
E = 1588
N = 1588 + NAT
X = 1588 + Corrosion Resistance
Note:
Group 1 SKUs do not support NAT nor 1588
Group 2 SKUs support NAT and/or 1588

5.0 [redacted] SUPPORT REQUIREMENTS

Following is the Hardware / Software needed from [redacted] to test the CIP Enhancements:

- EN2T with firmware 4.003 and Build 501500 or most current.
- RSLogix5000 v19.01 or most current.

6.0 HARDWARE DEVELOPMENT

6.1 The following list defines the scope of Hardware design activities and the responsible party.

- Cisco is responsible for the design of the Camaro products, including:
  - Electrical and mechanical design of all switches in the portfolio.
  - Component selection and board layout.
  - Compliance with EMC, Safety, hazardous location, Ethernet/IP and IEEE 1588 protocol requirements.
- Cisco is responsible for the fabrication, assembly and test of prototypes, including:
  - Procurement of all prototype materials to meet the lead times for each build.

o Delivering to [redacted] the quantity of prototypes stated in Section 4.0 for the purpose of Product and System Integration Testing by [redacted].

· [redacted] is responsible for System Integration Testing and Acceptance Testing of the Pre-Pilot units.

6.2 Test reports and supporting documentation for Compliance purposes:

For purposes of the following section, “Outsourced Product” is intended to refer to Product samples built by Cisco for the purpose of Safety / Compliance testing and certification by outside agencies.

6.3 Outsourced Products Regulatory Considerations:

Outsourced products, where EMC certifications are within the scope of Cisco’s responsibilities, require further consideration with regards to test report form and additional supporting documentation. Although not all possibilities can be addressed herein, the basic considerations are as follows:

i) Whenever possible, Cisco agrees to provide the test report in ink-signed original and electronic form or solely in a secure electronic form (EDM, certified PDF, etc.). Where original or secure electronic forms are not possible or practical, Cisco shall provide an inksigned English original “Letter of Authenticity” (LoA) indicating that Cisco holds the original test report and the provided paper or unsecured electronic test report copy is a true and complete copy of the original.

ii) Whenever possible, the provided test reports shall reference both Cisco’s and [redacted] model number as the “Equipment Under Test” (EUT). When this is not possible, Cisco shall provide an ink-signed English original “Letter of Equivalency” (LoE) indicating that Cisco’s model number and the corresponding [redacted] model number are equivalent (i.e. a product variant).

iii) Where applicable, Cisco shall provide regulatory Declarations of Conformity (DoC) in English electronic copy form (e.g. EU CE, AUS C-Tick, FCC, etc.). The provisions of item (ii) above shall be utilized where the provided DoC references only Cisco’s model number.

iv) A “Right of Access and Copy” agreement (RoAC) shall be provided by Cisco in inksigned English original form, granting [redacted] specific rights of use, access, and copy with regard to Cisco’s EMC (and other) certification data. Examples of the LoA, LoE, and RoAC documents are available from [redacted] Product Certification Engineering department.

v) Outsourced Products Agency Considerations - It is recommended that Cisco provide the appropriate Multiple Listing (ML), Private Label Agreement (PLA) and agency application documents via electronic form (EDM, certified PDF, etc.). The submitter’s / applicant model(s) and listee’s model(s) shall be identified for correlation purposes.

7.0 SOFTWARE DEVELOPMENT

7.1 Software for the [redacted] Product shall be developed and fully tested by Cisco as follows:

• Cisco IOS Software with applicable modifications as set forth in the System Functional Specification (SFS).

• Cisco agrees to make available to [redacted] the following specifications to review and provide feedback:
– System Functional Specification (SFS)
– SW Functional Specification (SW FS)
– CIP Feature Spreadsheet
– NAT Functional Specification
• Cisco is primarily responsible for defining, documenting and executing the Software Functional Test Plan, including CIP, NAT, IOS Feature, System and Regression Testing.
• [redacted] to review and provide feedback of the CIP, NAT and Software Functional Test Plans and associated test results in a timely manner, as agreed by the parties.
• Cisco agrees to support development of the [redacted] Add-on Profiles (AOP).

8.0 USER DOCUMENTATION

8.1 [redacted] Documentation - General

The Cisco and [redacted] documentation groups will work together to produce the [redacted] versions of required documents. The Cisco documentation group will provide source files that the [redacted] documentation group may use to prepare documentation for their product. With the exception of Release Notes, Cisco will provide [redacted] with not less than two drafts of each document for review and feedback prior to delivery of the production release versions. [redacted] agrees to perform thorough reviews of each document and provide detailed feedback in a timely manner agreed to by both parties. [redacted] software and hardware documentation shall be posted to the [redacted] web site and not to the Cisco web site. [redacted] documentation shall have the [redacted] name and logo on it. The Cisco name and logo shall not be printed on [redacted] documentation. All documentation will be delivered in electronic form only unless otherwise noted. Device manager online help is part of the Device Manager GUI, embedded in the product. Ownership of the completed documentation and its contents is addressed in the Master Agreement. Following are details of the specific documents that will be produced for the Product.

8.2 Software Documentation Deliverables

i) Software Configuration Guide

The Cisco documentation group will produce the Cisco version of the Software Configuration Guide (SCG) that includes conceptual information about the software features and procedures for configuring them using the Command Line Interface (CLI). For features that are platform-independent and documented in IOS technology guides or feature modules, the SCG will provide a brief description and refer to IOS documentation on the Cisco web site. The Cisco documentation group will provide source files of the SCG in FrameMaker 7.2 format, with illustrations, to be imported by [redacted] prior to FCS. For subsequent software releases, Cisco will provide documentation source files only for new or modified features.

ii) Software Release Notes

Cisco publishes release notes for every release of software, including bug-fix only maintenance releases.

· Cisco will create release notes that include standard information pertaining to the release, such as open and resolved caveats, limitations, etc. Cisco will provide [redacted] a FrameMaker file version of the release notes prior to FCS.

· [redacted] documentation resources, working with technical experts, can determine how much of this information will be included in the [redacted] release notes. [redacted] Documentation Group will be responsible for creating, posting and maintaining the [redacted] version of the Release Notes.

· In the event of interim software releases with bug fixes for security problems or to resolve other open caveats, Cisco documentation will provide the new information to [redacted] as the FrameMaker file of the new Cisco release notes for [redacted] to use as appropriate.

iii) Command Reference and System Message Guide

For every major software release for the Cisco version of the switch, Cisco will publish or update the Cisco Command Reference and System Message Guide for the Cisco version of the switch. These documents will be posted on the Cisco web site. Cisco will provide the URLs for these documents to [redacted] for its technical support or other users of the command line interface to reference. There will be no [redacted] version of these documents.

8.3 HARDWARE DOCUMENTATION DELIVERABLES

i) Getting Started Guide (GSG):

· Cisco will provide the FrameMaker files and illustrations of the Cisco version of the GSG to [redacted] (along with any [redacted]-specific screen captures).

· Cisco will provide the Cisco source files at each of the Cisco review cycles.

· The source files will be uploaded to the shared FTP site. Cisco will notify [redacted] when the files are available.

· [redacted] will be responsible for its version of the Getting Started Guide and make it available to end users separately from the shipping product, if required.

· If there are changes or revisions at a later date, Cisco will provide a copy of the Cisco FrameMaker files with change bars to indicate those changes.

· [redacted] will be responsible for localizing the [redacted] version of the getting started guide as required.

ii) Regulatory Compliance and Safety Information (RCSI):

· Cisco will provide the FrameMaker file and illustrations of the Cisco version to [redacted].

· [redacted] will be responsible for creating its own version of the RCSI, if required.

· If [redacted] requires any additional warnings in their version, [redacted] will provide and insert those warning translations.

· [redacted] will be responsible for localizing the [redacted] version of the RCSI, if required.

iii) Hardware Installation Guide (HIG):

· Cisco will provide the FrameMaker files and illustrations of the Cisco version to [redacted].

· Cisco will provide source files at each of the Cisco review cycles.

· [redacted] will be responsible for its version of the hardware guide and will make it available to end users separately from the shipping product, if required.

· If there are changes or revisions at a later date, Cisco will provide a copy of the Cisco FrameMaker files with change bars to indicate those changes.

· [redacted] will be responsible for localizing the [redacted] version of the hardware guide if required.

8.4 [redacted] Printed Documents (to ship with the Product):

[redacted] printed documentation, which ships with the product shall have both a Cisco part number and a [redacted] publication number. The documentation will be printed by approved print vendors according to Cisco standard print specifications. [redacted] printed

documentation may include a product information sheet which provides basic safety and legal information and url pointers to the [redacted] website and End User License Agreement (EULA). Unless otherwise agreed by the parties, the documentation described in this section will be the only printed documents to ship with the Product.

8.5 Device Manager Online Help

The [redacted] Device Manager (DM) Online Help (OLH) content will be based on the Cisco version. The look and feel of the [redacted] DM OLH follow the Cisco guidelines outlined in the DM section of the SFS. This includes English and any language translations.

- Cisco will be responsible for content related to configuration, monitoring, and troubleshooting through the DM GUI.
- [redacted] will be responsible for providing content related to [redacted] specific product support, hardware information (as applicable), and [redacted] specific network information.
- [redacted] will provide the relevant and corresponding [redacted] URLs referenced in the DM online help.
- Cisco will include [redacted] in all technical reviews of the online help.
- [redacted] will have the opportunity to add or modify content as appropriate during the review cycles. [redacted] will provide review input within the mutually agreed review cycle.
- Cisco will check in the OLH files for the software builds.
- Cisco will provide a copy of the OLH files as content for other [redacted] documentation.
- Cisco will localize the Device Manager and OLH into French, Italian, German, Spanish-Latin America, Japanese, simplified Chinese, and Portuguese-Brazil.

8.6 Misc Documents

- Cisco will provide exterior only 3D views of all [redacted] 7000 HW configurations. These models are to be delivered as .stp (step) files not later than delivery of the final draft.
- [redacted] may request delivery of specific IOS documentation source files if a need is identified.

9.0 TRAINING

Cisco shall provide three (3) training sessions for the purposes of training [redacted] support personnel on the Product. Each training session will provide not less than eight (8) hours of combined instructor led classroom training and labs. The training shall be conducted at a location in the United State mutually agreed to by the parties and may be videotaped by [redacted]. [redacted] has the right to use such videotaped training to “train the trainer” in order to enable [redacted] to provide additional training to other [redacted] personnel as needed. The training shall be made available prior to AFC.

10. 0 Cisco Pre-release CIP Test plan and CIP Test Results

10.1 Cisco CIP Test Plan

Cisco will provide [redacted] with a CIP Test Plan according to the milestone schedule. The CIP Test Plan will include information sufficient for [redacted] to determine the intended test coverage with the goal of achieving 100% functional coverage as well as sufficient

boundary condition, errant condition, variant path, and interrupted path testing to insure robust product operation. The Test Plan should list test cases, use cases, or general test coverage areas and may include test procedures. [redacted] will review the test plan and provide feedback to Cisco in a timely manner (as agreed between the parties) regarding functional areas not covered or lack of coverage for non-functional tests. Cisco agrees to make all reasonable commercial efforts to resolve any of [redacted] concerns with the CIP Test Plan.

10.2 Cisco CIP Test Results

Cisco CIP Test Results will include a list of test cases or use cases executed and the results of those tests. For each case, this document shall show the pass/fail criteria and result for that test. A new set of results will be expected for each regression of the test. Cisco will provide the test results and [redacted] will review the test results and provide feedback in as timely manner as agreed by the parties. Cisco agrees to make all reasonable commercial efforts to resolve any of [redacted] concerns with the CIP Test Results prior to delivery of Pilot units for Acceptance Testing.

10.3 Subsequent testing by [redacted] Automation

Cisco will provide [redacted] with the committed number of Pre-Pilot (PP) protos following completion of Cisco's Functional System Testing. [redacted] will run a series of acceptance and characterization tests on the PP protos provided by Cisco. [redacted] may choose to run other tests as deemed necessary and will make all reasonable commercial efforts to complete the testing in a timely manner. Cisco shall be allowed to release its own version of the Product to production upon completion of Cisco's internal qualification testing and will not be inhibited from doing so because [redacted] has not completed Acceptance Testing.

10.4 Defect tracking and correction process

[redacted] will validate Cisco's test results using the prototype and software images provided by Cisco. As a part of this testing, [redacted] will characterize any defects found and provide detailed descriptions of their findings to Cisco. [redacted] will provide support to reproduce the anomaly at the Cisco site if needed. Cisco will correct the defects and perform regression testing to confirm the defect has been resolved. Cisco will return corrected protos or provide software updates to [redacted], along with a description of the changes and regression test results. [redacted] will re-run the same tests which reproduced the defect to verify the corrective actions were effective. Regular Defect Resolution Meetings (DRM's) will be held during the testing phases between representatives of [redacted] Product Management, Project Management, Test and Development Engineering teams and the corresponding representatives at CISCO, referred to as the Defect Resolution Team (DRT). The DRT will use these meetings to classify defects as either:

- **Critical** – Anomalies that must be corrected prior to AFC release of the product.
- **Non-Critical** – Anomalies that may be deferred to a later firmware release.

Any disagreement in classification or specific corrective actions that cannot be resolved by the DRM in a timely manner will be escalated to the Cisco and [redacted] Executive Sponsors for resolution.

11.0 PRODUCT ACCEPTANCE

Acceptance of the Product shall mean conformance of the Pre-Pilot units to all material requirements of the Technical Specification shared with [redacted] as demonstrated by successful completion of Functional Certification Testing by Cisco and documented by associated Test Results supplied to [redacted] for their review and Acceptance.

P2 Prototypes will be delivered to [redacted] for the purpose of developing test beds and System Validation Testing environments, but no official acceptance testing will be conducted until Cisco has delivered fully operational and validated Pre-Pilot units.
In order to meet the delivery schedules set forth in Section 13 below, [redacted] shall perform its Acceptance Testing within 15 business day following delivery of Pre-Pilot units. The test duration may increase up to 30 business days based on the initial results of System Validation Testing. [redacted] acknowledges that an increase in test duration will likely have an impact on the overall Product development schedule and AFC date. In the event the Pre-Pilot units do not conform to the Specifications, [redacted] shall provide written notice to Cisco describing the deficiencies in sufficient detail to allow Cisco to reproduce the deficiencies in such units. If mutually agreed as being required, [redacted] will provide on-site support to enable Cisco to reproduce the issue. Cisco shall exert reasonable commercial efforts to correct the deficiencies so that the Product within the period of time mutually agreed upon by the parties.
Final approval of the Product by [redacted] shall be based on written Acceptance of the Pre-Pilot units, which may include agreement on a plan and schedule to correct deficiencies identified during the course of [redacted] Acceptance Testing and integration with the RSLogix 5000 AOP.
[redacted] shall provide Cisco with a written Letter of Acceptance or Rejection following completion of [redacted] Acceptance Testing and review of Cisco's test data. The Product shall be deemed accepted by [redacted] if [redacted] does not reply to Cisco within 5 business days following the completion date of [redacted] Acceptance Testing. In the event [redacted] issues a final rejection of the Product following a reasonable number of attempts by Cisco to correct deficiencies, then [redacted] may terminate this Statement of Work by providing written notice to Cisco.

12.0 PROGRAM MILESTONES / DELIVERABLES SCHEDULE

The following table contains target dates for key milestones and deliverables that shall be tracked during development of the Product. The dates are non-binding forecasts to be used for planning purposes and are subject to change. Cisco will updated versions of the schedule on a regular basis and provide more specific dates as they get closer.

#	Hardware Development Deliverables / Milestones	Target Date
H1	P1B (Group 1) - Protos received at Cisco	May 2011
H2	P1B (Group 2) - Protos received at Cisco	July 2011
H3	P1B – Tested Protos shipped to RA	September 2011
H4	P1B – HW Validation Testing Complete	October 2011
H5	P2 - First protos received at Cisco	November 2011
H6	P2 - Tested Prototypes shipped to RA	January 2012
H7	P2 - HW Validation Testing at Cisco complete	February 2012
H8	PP – First protos received at Cisco	February 2012
H9	PP - Tested units shipped to RA	March 2012
H10	Start of Pilot build	March 2012
H11	Pilot units shipped to RA	April 2012
H12	Completion of Final Acceptance Testing by RA	April 2012
H13	Letter of Product Acceptance issued by RA	May 2012

	Software Development and Test Deliverables / Milestones	
S1	CIP Enhancements – First draft of Functional Spec available for review	May 2011
S2	CIP Enhancements – Final draft of Functional Spec available for review	June 2011
S3	CIP Enhancements – First draft Test Plan available for review	May 2011
S4	CIP Enhancements – Final draft Test Plan available for review	June 2011
S5	CIP Features – Initial Test results	November 2011
S6	CIP Features – Final Test results	January 2012
S7	CIP Certification issued by ODVA	March 2012
S8	NAT – First draft of Functional Spec available for review	April 2011
S9	NAT – Final draft of Functional Spec available for review	May 2011
S10	NAT – First draft Test Plan available for review	June 2011
S11	NAT – Final draft Test Plan available for review	June 2011
S12	NAT – Initial Test results	November 2011
S13	NAT – Final Test results	January 2012
S14	System SW – First draft of SW FS available for review	May 2011
S15	System SW – Final draft of SW FS available for review	June 2011
S16	System SW – Start of SW Functional Testing on P1B Protos	July 2011
S17	System SW – Completion of SW Functional Testing on P1B Protos	November 2011
S18	System SW – Start of SW Functional Testing on P2 Protos	November 2011
S19	System SW – Completion of SW Functional Testing on P2 Protos	February 2012
S20	System SW – Release of Production SW Image to Cisco website	March 2012

	Compliance/Safety Testing Deliverables / Milestones	
C1	Completion of Safety and Compliance testing on P1B Protos	October 2011
C2	Completion of Safety and Compliance testing on P2 Protos	February 2012
C3	All Safety and Compliance certificates issued	April 2012

	Documentation Deliverables / Milestones	
D1	First draft of GSG delivered to RA for available for review	January 2012
D2	Final draft of GSG delivered to RA for available for review	February 2012
D3	Final RA customized Document files delivered to Cisco for production release	March 2012
D4	First draft of Hardware Installation Guide (HIG) delivered to RA for review	December 2011
D5	Final draft of Hardware Installation Guide (HIG) delivered to RA for review	January 2012
D6	Final HIG delivered to RA for customization and production release	February 2012
D7	Cisco version of release notes delivered to RA for customization and production release	March 2012
D8	Online Help (final draft) delivered to RA for Review	February 2012
D9	Final Online Help files delivered to RA for customization and production release	March 2012
D10	First draft of IOS Software Configuration Guide delivered to RA for review	December 2011
D11	Final draft of IOS Software Configuration Guide delivered to RA for review	February 2012

Exhibit F – Jointly Developed Technology

All ideas, concepts, designs, technical information, algorithms, formulas, specifications and inventions (whether or not patentable and whether or not reduced to practice) relating to the password security mechanism as described in Section 6 of the CIP Ethernet/IP Software Functional Specification (included in as Appendix C of the ([redacted] 8000) Xmen2 External System Functional Specification), excluding any computer code written or created by either party relating to the foregoing, which computer code shall be deemed to be the sole property of the party which wrote or created such code.

All ideas, concepts, designs, technical information, algorithms, formulas, specifications and inventions (whether or not patentable and whether or not reduced to practice) relating to the parameter object as described in Section 5.2.1 and Exhibit A of the CIP Ethernet/IP Software Functional Specification (included in as Appendix C of the ([redacted] 8000) Xmen2 External System Functional Specification), excluding any computer code written or created by either party relating to the foregoing, which computer code shall be deemed to be the sole property of the party which wrote or created such code.

All ideas, concepts, designs, technical information, algorithms, formulas, specifications and inventions (whether or not patentable and whether or not reduced to practice) relating to the vendor specific extensions of the Ethernet link object as described in Section 5.2.9 and Exhibit A of the CIP Ethernet/IP Software Functional Specification (included in as Appendix C of the([redacted] 8000) Xmen2 External System Functional Specification), excluding any computer code written or created by either party relating to the foregoing, which computer code shall be deemed to be the sole property of the party which wrote or created such code.

All ideas, concepts, designs, technical information, algorithms, formulas, specifications and inventions (whether or not patentable and whether or not reduced to practice) relating to the vendor specific extensions of the Ethernet identity object as described in Section 5.2.5 and Exhibit A of the CIP Ethernet/IP Software Functional Specification (included in as Appendix C of the ([redacted] 8000) Xmen2 External System Functional Specification), excluding any computer code written or created by either party relating to the foregoing, which computer code shall be deemed to be the sole property of the party which wrote or created such code.

All ideas, concepts, designs, technical information, algorithms, formulas, specifications and inventions (whether or not patentable and whether or not reduced to practice) relating to the I/O and configuration assemblies, including the data structures and the security behavior associated with the password in the configuration assembly, as described in Section 5.2.2 of the CIP Ethernet/IP Software Functional Specification (included in as Appendix C of the ([redacted] 8000) Xmen2 External System Functional Specification), excluding any computer code written or created by either party relating to the foregoing, which computer code shall be deemed to be the sole property of the party which wrote or created such code.

All ideas, concepts, designs, technical information, algorithms, formulas, specifications and inventions (whether or not patentable and whether or not reduced to practice) relating to the Device Manager CIP status page as described in Appendix D – [redacted] Automation Device Manager of the ([redacted] 8000)Xmen2 External System Functional Specification, excluding any computer code written or created by either party relating to the foregoing, which computer code shall be deemed to be the sole property of the party which wrote or created such code.

The items as described in Appendix D under the heading style guidelines and Mockup – [redacted] Automation Device Manager of the ([redacted] 8000)Xmen2 External System Functional Specification taken as a whole, and not with respect to individual components thereof, shall be deemed to constitute the [redacted] "Look and Feel" of the [redacted] Device Manager and, as such, shall be deemed to constitute [redacted] pre-existing intellectual property right.

e CISCO

Document Number	EDCS-982269
Based on Template	EDCS-189226 Rev 31
Created By	[redacted]
Program Manager	

Stratix 7000
System Functional Specification

[redacted]7000is anIndustrial Ethernet access product family based on Cisco Sytem's IE2000 Ethernet Switch family, which is targetedforEthernet based networks in manufacturing, industrial and other harsh environments. The Cisco internal project name is [redacted]

Reviewers

Department	Name/Title
Development Engineering	[redacted]
DevTest Engineering	
Customer Value Chain Management	
Product Marketing	
Customer Advocacy	
Compliance	
Program Management	
Corporate Compliance Accessibility Group	

Modification History

Revision	Date	Originator	Comments
1	[redacted]		First draft
2			Made a few changes, realized not using correct template, will import HW sections to SFS after SW inputs using new template
3			Initial version – Use new CPDM SFS template. Added most SW features
4			Update SW sections: MIB, Egress Rate Limiting, NAT, RSTP/MST, CIP, Added sections: Cable Diagnostics, Smartport templates
5			Added Hardware Sections
6			Updated SW section network management and remove changes bar. Added section OBFL, download recovery and TDR.
7			Further HW updates
8			Held HW sections review, added comments per review inputs
9			Removed NW mgt requirements (this should be done by NW mgt team). Removed L2 enhancements sections since we can

			leverage of from other projects. Updated sections 2.3.8 - 2.3.10, 2.3.12.
10			Updated section 2.7 "Manufacturing Considerations".
11			Updated section 5.4 "Sole / Single Source Components".
12			Update SW sections upon Review comments (Jan. 18, 2011)
13			Misc updates based on personal review
14			Update based on Jaime's review comments. Fill in sections 3 and 4 for software. Move some table, paragraphs from section 2 to sections 3 and 4. There is no change in the basic content to section 2, except section 2.3.10.8 (more detail added to feature req based on meeting with Rockwell Jan 25)
17			Updated Section 2.7 "Manufacturing Considerations".
18			Updated SW sections 2 and up to section 3.2 based on Jon Harrod comments for clarity.
19			Added sections 2.3.13, 2.3.14. Updated section 3.4
20			Minor cleanup and corrections Header, section 6 and 7 page breaks between block diagrams
21			Updated section 3.6 (put back the gap analysis table and add comment), Updated section 3.11 (Serviceability requirement) , 4.6 (memory estimate).
22			Additional updates to section 3.11 and section 5
23			Added statement that support MIBs are READ-ONLY
24			Added Mechanical section 3.8
25			Modified section 2.3.14 as discussed with diag, marketing, and SW
26			Basic cleanup
30			Changes from Review
31			Updated 2.3.8 based on review feedback
32			Minor text edits to match cleanup in External SFS
33			Updated SFP tables, section 3.5
34			Added late review comments from Prince
35			Updated Compliance section, Marine, no IE3K references
36			Fixed numbering problem in compliance section Cleaned up tables that were wider than the sheet.
37			Added corrosion testing and new MTBF numbers
38			Updated accessibility section based on review feedback
39			Updated compliance section for corrosion testing. Updated alarm section Other minor clarifications based on RA feedback
40			Updates after first review with RA
41			Updated section 2.1.2 and 2.3.6 based on minutes from Camaro SFS Q&A with [redacted] (March 15, 2011)
42			Updates after second review from [redacted]
43			Updated LED table, section 2.2.4.6
44			Updated Shock & Vibration table 3.9.1
45			Updated box sizes in table in section 2.2.1.1
46			Updated LED info. Added mechanical drawings with DIN rail
47			Updated Items 31, 32, 38, 42, 46, 48, 50, 52, 58, 61, 63, 77, 79-82, 87, 88, 93, 100, 103, 121 based on SFS_Review_Mtg_Actions.xls Added comment in section 2.3.14 – Camaro operates ONLY Cisco SD card.
48			Updated section 2.3.13
49			Addressed [redacted] AIs 25, 102, 104, 107 Reworded section 4.8
50			Updated [redacted] AIs 8, 31, 32, 38, 42, 46, 52, 63, 66, 77, 81, 84, 100, 127 based on Jon's review

			Updated 2.1.2
51			Updated [redacted] AI 20 (added section 2.3.15)
52			Updated LED section with [redacted] LEDs Updated section 3.13 based on [redacted] feedback
53			Updated section 2.2.4.8 , updated SD Card cover statement
54			Updated Table in 2.1 to remove [redacted] PIDs Added CSA C22.2, No 213 to compliance section
55			Clarified section/table 2.1.1
56			Updated size table and DIN rails sizes on page 55, and sections 3.8-1-3.8.4
57			Updated Product Renderings/Eliminated mechanical disclaimer
58			Bad check-in
59			Updated [redacted] AI 20, 35, 63, 84, 93, 100
60			Fixed Table in 2.2.1.1 - 2.2.1.4 - Sizes to match 3.8
61			Updated RA AI 104 and 139
62			Updated section 2.2 cleaned up mounting options descriptions
61			Section 3.9.1, updated non-op shock
62			Updated section 2.3.9, NAT 2.1 from 4 to 128 vlans
63			Updated section 2.3.15. alarm out relay default to de-energized
64			Updated section 2.2.4.5, alarm out relay Updated section 3.2.1; Added DHCP snooping feature to IE Lite
65			Updated sections 2.3.6, 2.3.9, and 2.3.15
66			Updated table in section 2.3.15
67			Updated [redacted] SKUs
68			Final version of Stratix 7000 SFS - Changed title on page 1 from [redacted] 7000 Changed header to match new title and corrected EDCS number Removed all attached emails and review action item trackers (replaced by AI Tracker - EDCS-995897). Removed reference documents that are not included per the SOW.
69			Deleted image of [redacted] Minor changes to introduction.
70			Removed CIP Initial Configuration requirement based on RA request.
71			Moved alarm table from section 2.4.1 to section 2.3.15

Table of Contents

1 Purpose

The purpose of this document is to provide a high level overview of design considerations for the [redacted] program. This document includes both hardware and software design considerations. This document will not address cost, schedule, or program risk. It also gives some detail about specifics of the design implementation.

1.1 Scope

This document covers the [redacted] project, which are Industrial Automation products. It consists of a family of 19 switches, ranging from 6 ports to 20 ports. There are four switch chassis form factors.

The requirements specify the behavior of the system as seen by the end user. They do not specify "how" the system will be built except for necessary constraints on the design such as needed interfaces to other systems or valid constraints on size, shape, processor and memory utilization, power consumption, etc. The behavior may be described in terms of how the system enables the end user to perform work (i.e., the functions, performance, quality requirements, etc).

The architectural design describes the components of the system, their individual functions and performance, and how they interface with each other.

Development considerations such as schedule, cost, development process, and staffing are not included in a system specification.

							Factory Defaults			
Cisco PID	Rockwell PID	Downlinks	Uplinks (Fixed RJ45)	Uplinks (Fixed SFP)	Combo Uplinks (SFP/RJ45)	FPGA (1588/NAT)	Lite	Base	Conformal Coating	Power
IE-2000-4TS-L	1783-BMS06SL	4		2 100Mb		No	STD	Upgrade*	No	DC (12, 24, 48 V)
IE-2000-4TS-B	1783-BMS06SA	4		2 100Mb		No	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-4T-L	1783-BMS06TL	4	2 100Mb			No	STD	Upgrade*	No	DC (12, 24, 48 V)
IE-2000-4T-B	1783-BMS06TA	4	2 100Mb			No	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-4TS-G-L	1783-BMS06SGL	4		2 Gig		No	STD	Upgrade*	No	DC (12, 24, 48 V)
IE-2000-4TS-G-B	1783-BMS06SGA	4		2 Gig		No	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-4T-G-L	1783-BMS06TGL	4	2 Gig			No	STD	Upgrade*	No	DC (12, 24, 48 V)
IE-2000-4T-G-B	1783-BMS06TGA	4	2 Gig			No	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-8TC-L	1783-BMS10CL	8			2 100Mb	No	STD	Upgrade*	No	DC (12, 24, 48 V)
IE-2000-8TC-B	1783-BMS10CA	8			2 100Mb	No	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-8TC-G-L	1783-BMS10CGL	8			2 Gig	No	STD	Upgrade*	No	DC (12, 24, 48 V)
IE-2000-8TC-G-B	1783-BMS10CGA	8			2 Gig	No	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-8TC-G-E	1783-BMS10CGP	8			2 Gig	1588	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-8TC-G-N	1783-BMS10CGN	8			2 Gig	1588 and NAT	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-16TC-L	1783-BMS20CL	16		2 100 Mb	2 100 Mb	No	STD	Upgrade*	No	DC (12, 24, 48 V)
IE-2000-16TC-B	1783-BMS20CA	16		2 100 Mb	2 100 Mb	No	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-16TC-G-L	1783-BMS20CGL	16		2 100 Mb	2 Gig	No	STD	Upgrade*	No	DC (12, 24, 48 V)
IE-2000-16TC-G-E	1783-BMS20CGP	16		2 100 Mb	2 Gig	1588	N/A	STD	No	DC (12, 24, 48 V)
IE-2000-16TC-G-X	1783-BMS20CGPK	16		2 100 Mb	2 Gig	1588	N/A	STD	Yes	DC (12, 24, 48 V)

2 Functional Overview

[redacted] is an Industrial Ethernet Access family of switches. It is designed for interconnecting in the manufacturing factory environment as part of Industrial Automation.

2.1 System Overview

The [redacted] product family has 19 SKUs, but each SKU can be packaged with Cisco front panel overlays, or with [redacted] front panel overlay for a total of 38 possible SKUs, which manufacturing will have to manage. For many of these SKUs the difference is very slight, such as a different Board ID or a different version of IOS image loaded. The following PID table was derived from the PID table listed in the PRD, but is color coded to show which SKUs are supported by which hardware configurations.

HW Configuration/Name	Boards	PCB Assy	Cisco PID
#1/	backplane	Chas3	
	power	V6	
	CPU	Zeta	IE-2000-4T-B/L
Camaro-Z4	Port	Coupe	IE-2000-4T-G-B/L
#2/	backplane	Chas3	
	power	V6	
	CPU	Zeta	IE-2000-4TS-B/L
Camaro-Z4S	Port	CoupeS	IE-2000-4TS-G-B/L
#3/	backplane	Chas3	
	power	V6	
	CPU	Zeta	IE-2000-8TC-B/L
Camaro-Z8	Port	Hatch	IE-2000-8TC-G-B/L
#4/	backplane	Chas3	
	power	V8	
	CPU	Zeta+	IE-2000-8TC-G-E
Camaro-Z8E	Port	Stretch	IE-2000-8TC-G-N
#5/	backplane	Chas4	
	power	V8	
	CPU	Zeta+	IE-2000-16TC-B/L
	Port	Stretch	IE-2000-16TC-G-L
Camaro-Z16E	Expansion	Limo	IE-2000-16TC-G-E
#6/	same as #5 except must meet corrosive gas tests		
Camaro-Z16E			IE-2000-16TC-G-X

2.1.1 HW Overview

All 38 SKUs can be reduced to 5 fundamental HW models. The following table lists the different HW

configurations. (Only the primary Cisco SKU is given.)

The [redacted] HW configurations will consist of the following:

Cisco SKU PID	Code Name	Description
IE-2000-4T-G	[redacted]Z4G	4 10/100 FE Copper + 2 10/100/1000 GE Copper ports
IE-2000-4TS-G	[redacted]Z4SG	4 10/100 FE Copper + 2 GE SFP fiber ports
IE-2000-8TC-G	[redacted]Z8G	8 10/100 FE Copper + 2 GE combo ports
IE-2000-8TC-G-E	[redacted]Z8GE	8 10/100 FE Copper + 2 GE combo ports + FPGA
IE-2000-16TC-G-E	[redacted]Z16GE	16 10/100 FE Copper + 2 GE combo + 2 100FX SFP fiber ports + FPGA

2.1.2 SW Overview

Many of the [redacted] SKU's will support both aBase and Light version of IOS. Other IOS features such as GE uplink ports and 1588/NAT functionality will key off the Board ID. The [redacted] Automation and Cisco versions will run the same IOS image. There will be a protection mechanism to make sure that the [redacted] Automation boxes will behave as [redacted] boxes and Cisco boxes will behave as Cisco boxes. The following table lists software images:

Cisco PID	[redacted] PID	Factory Default IOS	
		Lite	Base
IE-2000-4TS-L	1783-BMS06SL	STD	Upgrade*
IE-2000-4TS-B	1783-BMS06SA	N/A	STD
IE-2000-4T-L	1783-BMS06TL	STD	Upgrade*
IE-2000-4T-B	1783-BMS06TA	N/A	STD
IE-2000-4TS-G-L	1783-BMS06SGL	STD	Upgrade*
IE-2000-4TS-G-B	1783-BMS06SGA	N/A	STD
IE-2000-4T-G-L	1783-BMS06TGL	STD	Upgrade*
IE-2000-4T-G-B	1783-BMS06TGA	N/A	STD
IE-2000-8TC-L	1783-BMS10CL	STD	Upgrade*
IE-2000-8TC-B	1783-BMS10CA	N/A	STD
IE-2000-8TC-G-L	1783-BMS10CGL	STD	Upgrade*
IE-2000-8TC-G-B	1783-BMS10CGA	N/A	STD
IE-2000-8TC-G-E	1783-BMS10CGP	N/A	STD, 1588
IE-2000-8TC-G-N	1783-BMS10CGN	N/A	STD, 1588, NAT
IE-2000-16TC-L	1783-BMS20CL	STD	Upgrade*
IE-2000-16TC-B	1783-BMS20CA	N/A	STD
IE-2000-16TC-G-L	1783-BMS20CGL	STD	Upgrade*
IE-2000-16TC-G-E	1783-BMS20CGP	N/A	STD, 1588

IE-2000-16TC-G-X	1783-BMS20CGPK	N/A	STD, 1588

NOTE: * The [redacted] version will not have the software license upgrade capability initially since [redacted] SKUs will not have the license infrastructure in place. This restriction is to avoid the backward incompatibility between the initial IOS release and the new [redacted] SKUs which have the licensing support. This is taken from the PRD.

2.2 Feature List (Hardware)

Due to the number of different SKUs in the Camaro product family, differentiating features will be described in following sections. The following HW features are common to all SKUs in Camaro family.

Feature	Marketing Request	Engineering Response
Ventilation: No fans, no other special restrictions.	Required	Yes for -40 to 60C 75C is achievable is a NEMA TS-2 compliant installation with a fan or blower equipped enclosure, 100 CFM minimum airflow
DC Power: • Dual feed • ±9.5 to 60 VDC	 Required Required	 Yes Yes
Cabling Options: • All skus support front cabling	Required	Yes
Flash: Enough to support 2 full IOS images for life of the product	Required	Yes, 64MB
DRAM: 128MB minimum, does not mention ECC.	Required	Yes, 128MB or 256MB ECC will be supported.
Hot Swappable FlashDrive:	Required	Yes, SD flash will be supported.
1588v2 Support: • All ports	Desired	Yes (on certain skus)
NAT Support	Desired	Yes (on certain skus)
Temperature Sensor	Required	Yes
Front Recessed Setup Button	Required	Yes
Cable Diagnostics	Required	Yes
Ground Lug: Cable side	Required	Yes

Management Port: Serial RS232 USB	 Required Desired	 Yes Yes
Alarm Contacts: alarm output(s) alarm input(s)	 Required 1 Required	 Yes, 1 Yes, 2
Dying Gasp:	No requirement	No
OBFL:	Required	Yes, HW supports Temperature monitor
LED Indicators: Require fault indicators for power supply and system, alarm status, and per port status.	Required	Yes
Air Flow: Convection	Required	Yes, No fan.
Support following SFPs: **Industrial Grade:** 1) GLC-FE-100LX-RGD= (SM) 2) GLC-FE-100FX-RGD= (MM) 3) GLC-SX-MM-RGD 4) GLC-LX-SM-RGD 5) GLC-ZX-SM-RGD 6) Commercial SFPs	Required	Yes (See section 3.5 for full list of SFPs supported) (Commercial SFPs will have a restricted operating temperature range)
Brand Protection	Required	Yes
Observed MTBF: • All: The MTBF target is 42.7 Years or 374,052 hours.	Required	This is the design goal
Mounting options: All SKUs: Rack, Wall and DIN Rail	Required	Yes DIN rail mounting natively. Rack mounting requires optional bracket. Wall mounting supported through add-on bracket.
Operating Temperature: -40 to +75C	Required	-40° to +75°C achieved with 100CFM blower in TS-2 cabinet Sectiont 3.9.1 details the temp specs
Storage Temperature: -40° to +85°C	Required	Yes
Operating Relative Humidity: 5% to 95%, non-condensing	Required	Yes
Storage Environment: Temperature: -40° to 85°C	Required	Yes

Altitude: 15,000 feet (4570 meters)		

2.2.1 Hardware Features – Unique System Configurations

Hardware features unique to each system configuration are described in the following sections.

2.2.1.1 Camaro-Z4G and Camaro-Z4SG Feature List

The [redacted]-Z4G and [redacted]-Z4SG have the lowest port count and smallest chassis size of the Camaro family of products. [redacted]-Z4G has all copper ports, [redacted]Z4SG has SFP connectors for fiber interfaces. These switches will have the same form factor.

Feature	Marketing Request	Engineering Response
Camaro-Z4G:4 10/100 FE copper ports + 2 10/100/1000 GE copper ports	Required	Yes
Camaro-Z4SG: 4 10/100 FE copper + 2 100/1000SFP ports	Required	Yes
Chassis Size Matches Table in Section 3.8	Required	**Width:** Yes **Height:** Yes **Depth:** Yes

Each of these switches can be software limited to 100Mbit via BoardID value. (SW will use this to create the 100MB only skus.) Also each of these can be loaded with either Base or Light version of IOS. Therefore these HW models support the first 8 Cisco SKUs listed in the PRD PID table (16 SKUs total including Rockwell Automation versions).

2.2.1.2 Camaro-Z8G Feature List

[redacted]-Z8G is a 10 port design and is the low end intermediate port count portion of the family.

Feature	Marketing Request	Engineering Response
[redacted]**-Z8G:** 8 10/100 FE copper + 2 GE combo (copper orSFP) ports	Required	Yes
Chassis Size Matches Table in Section 3.8	Required	**Width:** Yes **Height:** Yes **Depth:** Yes

This switch can software limit the combo ports to 100Mbit via BoardID value. Also each of these can be loaded with either Base or Light version of IOS. Therefore this HW model supports the next 4 Cisco SKUs listed in the PRD PID table (8 SKUs total including [redacted] versions).

2.2.1.3 Camaro-Z8GE Feature List

[redacted]-Z8GE is a 10 port switch with an intermediate port count but with the added functionality of 1588 and NAT to the Camaro family.

Feature	Marketing Request	Engineering Response
[redacted]Z8GE: 8 10/100 FE copper + 2 GE combo (copper orSFP) ports +1588/NAT FPGA	Required	Yes
Chassis Size Matches Table in Section 3.8	Required	**Width:** Yes **Height:** Yes **Depth:** Yes

This switch does not software limit the combo ports to 100Mbit. There are two software versions, one with 1588 support and one with both 1588 and NAT. Therefore this HW model supports the next 2 Cisco SKUs listed in the PRD PID table (4 SKUs total including Rockwell versions).

2.2.1.4 [redacted]-Z16GE Feature List

Camaro-Z8G is a 20 port switch with a high port count with the added functionality of 1588 and NAT. This is the top end portion of the Camaro family.

Feature	Marketing Request	Engineering Response
[redacted]Z16GE: 16 10/100 FE copper + 2 GE combo (copper orSFP) ports +1588/NAT FPGA + 2 100FX SFP ports	Required	Yes
Chassis Size Matches Table in Section 3.8	Required	**Width:** Yes **Height:** Yes **Depth:** Yes

This switch has several HW options determined via BoardID value and IOS image loaded. NAT is not supported on any of these switches, but that is a marketing decision and not a HW limitation. Therefore this HW model supports the next 4 Cisco SKUs listed in the PRD PID table (8 SKUs total including [redacted] versions).

The final switch is identical to the previous switch except the PCB assemblies are conformal coated if required.

Feature	Marketing Request	Engineering Response
Conformal Coating	Required	Conformal Coating will be used if required to pass required compliances. (see section 3.9.1.4)

This HW model supports the last Cisco SKUs listed in the PRD PID table (2 SKUs total including [redacted] versions).

2.2.2 Description – System Configurations

Camaro systems SKUs will each consist of:

1. Power board,
2. CPU board,
3. at least 1 Port board, and
4. Backplane board.

System configurations are determined by which PCB assemblies are combined together.

2.2.2.1 Camaro system PCBs

There are a total of 14 PCBs required to meets all system requirements, here is a list:

Assy #	Name	Description	Size/Layers/Technology
73-13835-xx	v6	small power board (under 20W)	4.75" x 3.8" x.062", 8L standard, 64 pin gold edge fingers
73-13679-xx	v8	larger power board (under 36W)	4.75" x 4.8" x.062", 8L standard, 64 pin gold edge fingers
73-13680-xx	zeta	small form factor CPU board	4.75" x 3.8" x.062", 12L standard, 98 pin gold edge fingers
73-13837-xx	zeta+	larger form factor CPU board	4.75" x 4.8" x.062", 12L standard, 98 pin gold edge fingers
73-13687-xx	coupe	port board, 4FE + 2 GE, all copper	4.75" x 3.8" x.062", 10L standard, 98 pin gold edge fingers
73-13725-xx	coupeS	port board, 4FE + 2 GE SFP	4.75" x 3.8" x.062", 10L standard, 98 pin gold edge fingers
73-13681-xx	hatch	port board, 8FE + 2 GE combo	4.75" x 3.8" x.062", 10L standard, 98 pin gold edge fingers
73-13682-xx	stretch	port board, 8FE + 2 GE combo +FPGA	4.75" x 4.8" x.062", 14L HDI, 98 pin gold edge fingers
73-13683-xx	limo	expansion port board, 8 FE + 2 100M SFP	4.75" x 4.8" x.062", 10L standard, 98 pin gold edge fingers
73-13723-xx	chas3	3 board backplane	
73-13724-xx	chas4	4 board backplane	
73-13684-xx	ss8	8 port sidactor protection board	
73-13836-xx	lugnut	dual SFP board used for combo ports	
73-14021-xx	alarm	Alarm I/O, used on zeta, zeta+	

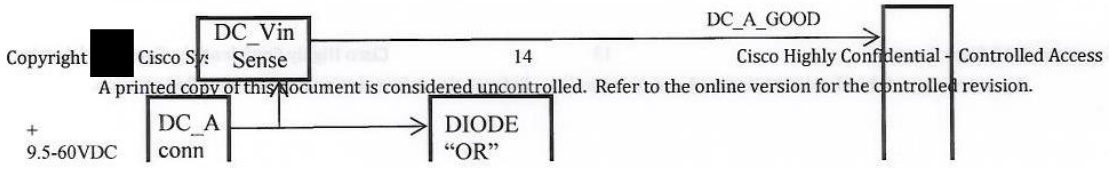
2.2.3 System Block Diagrams

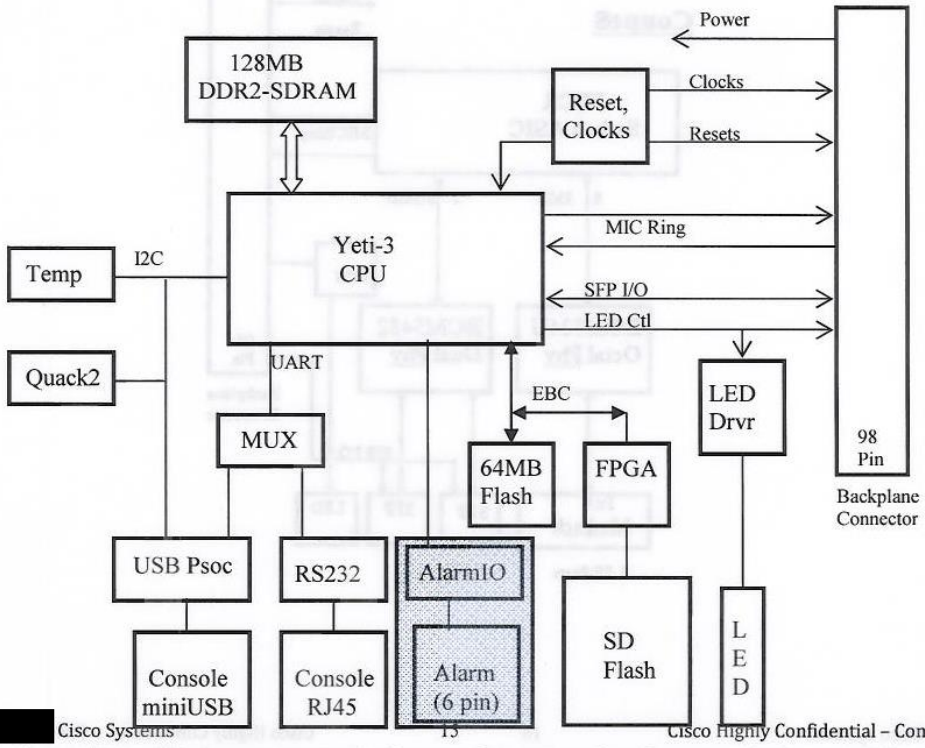
Camaro system SKUs are each comprised of a subset of above listed PCBs, the following examples show representative block diagrams.

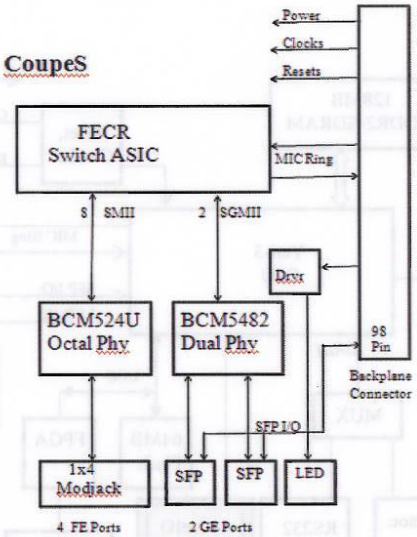
2.2.3.1 [redacted]-Z4SG Block Diagrams

This SKU consists of:

1. V6
2. Zeta
3. CoupeS
4. Chas3



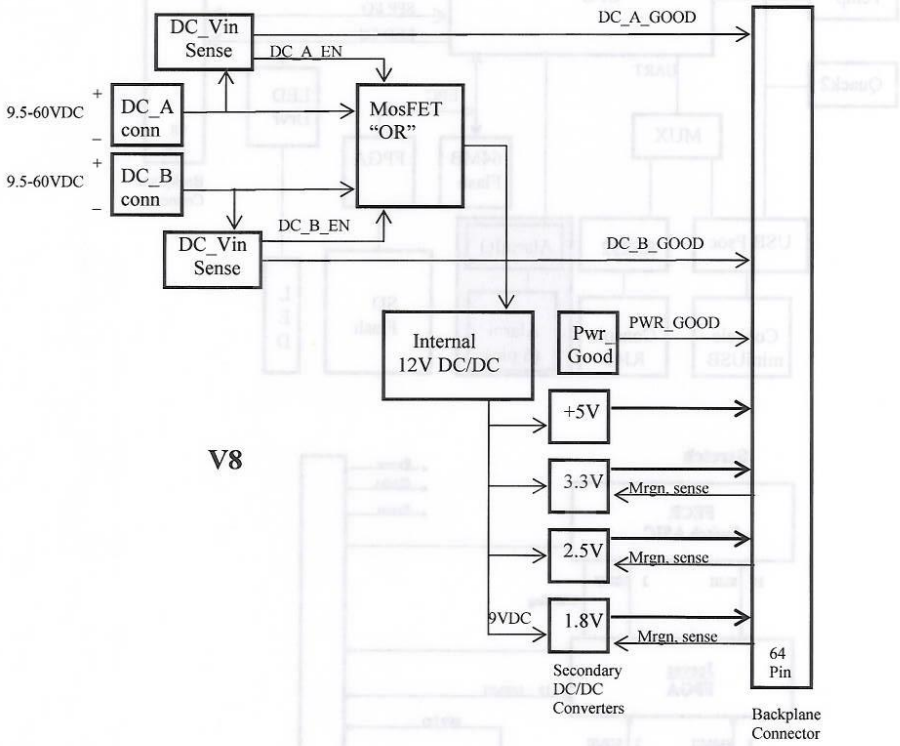




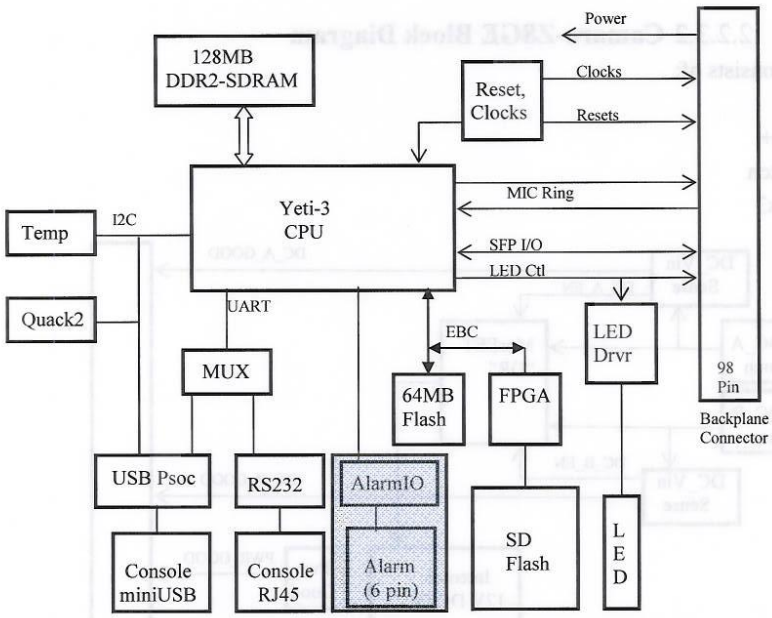
2.2.3.2 [redacted]-Z8GE Block Diagram

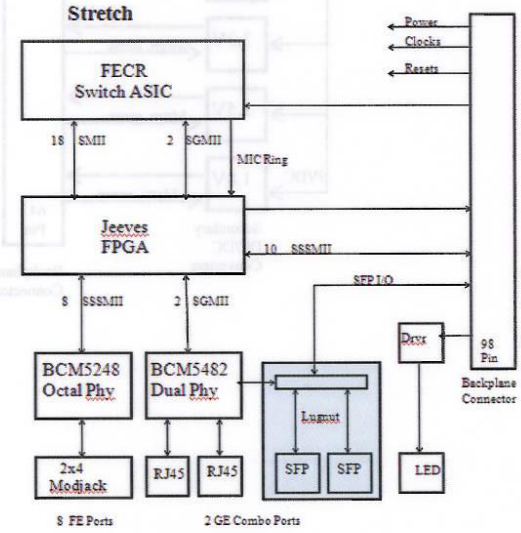
This SKU consists of:

1. V8
2. Zeta+
3. Stretch
4. Chas3



V8





2.2.4 External Interfaces

The following sections describe external interfaces on [redacted]

2.2.4.1 Ethernet Uplink Ports

[redacted]-Z4 supports two copper 10/100Base-T ports. Camaro-Z4G supports two copper 10/100/1000Base-T ports. [redacted]-Z4S supports two fiber 100Mb SFP ports. [redacted]-Z4SG supports two fiber 100Mb or 1000Mb SFP ports. The remainder of Camaro products support two combo ports. Combo ports support both copper and SFP interfaces, though only one interface can be used at a time. The hardware design supports 1G uplink ports. However, in some products this is limited to 100Mb via software. These ports support standard Ethernet features such as forced or auto-negotiating speed and duplex, auto-MDIX, and cable diagnostics.

2.2.4.2 10/100 Ethernet Downlink Ports

[redacted] supports 10/100Base-T ports. These ports support standard Fast Ethernet features such as forced or auto-negotiating speed and duplex, auto-MDIX, and cable diagnostics.

2.2.4.3 Extra SFP Uplink Ports

[redacted]-Z16GE supports two additional 100Base-X SFP ports providing 4 uplink ports. These ports will not support the 1000Base SFPs.

2.2.4.4 Console Port

All [redacted] SKU's support twoconsole port connectors for management communication to the swith via a UART interface. If a USB console cable is detected, the USB console LED will turn on and the miniB-USB connector will be selected for console I/O. Otherwise the console I/O defaults to the standard RS232 UART connections of the RJ45 console connector. (Thus if cables are installed on both ports, the USB console port will take precedence.)

The USB connector will require a positive locking mechanism for the attached cable to meet the 15N pull requirement in hazardous locations.

2.2.4.5 Alarm Inputs/Outputs

All [redacted] SKU's support two dry contact alarm inputs and one alarm output relay. The contacts for both input and output alarms share a common Alarm connector.

Input Alarms:

Each of the two dry contact Alarm inputs can be provisioned separately to generate an alarm event. SW can be used to configure the alarm state as major or minor as well as setting the default state as open or closed. The User will be notified via alarm messages as well as LED indicators when an alarm triggers. The user is provided a single pin for each Alarm input as well as an Alarm Return pin on the Alarm Connector.

Output Alarm:

The Output Alarm uses a single form C relay and both the normally open and normally closed contacts are made available to the user along with the relay common contact. Please refer to section 2.3.15 for operational mode.

2.2.4.6 System and Port LEDs

All [redacted] SKU's have System LEDs to convey the overall system status and the power supply's input and output statuses. All skus also have per port LEDs to convey port status, and alarm output status.

Each combo port has two LEDs: one for the SFP and one for the RJ45 connector. The appropriate LED will be active to indicate the active media. There will be one LED per 10/100 port and SFP uplink port.

All LEDs are bi-color. Table 1 below explains the LED behaviors:

Table 1: [redacted] LED Behavior

LED:	LED Definition:	Notes
System	Off – System is not powered on.	Replaced by EIP ModStatus LED on RA skus
	Blinking Green – POST in progress	
	Solid Green – System is operating normally.	
	Solid Red – Switch is not functioning properly.	
DC_A DC_B	Off – Power is not present on the circuit, or the system is not powered up.	Same function and location on [redacted] SKUs
	Solid Green – Power is present on the associated circuit.	
	Solid Red – Power is not present on the associated circuit, and the switch is configured for dual-input power.	
Alarm Out	Off – Alarm Out not configured or the switch is off	Same function and location on [redacted] SKUs
	Solid Green – Alarm Out is configured, no alarm detected.	
	Blinking Red - Switch has detected a major alarm.	
	Solid Red –Switch has detected a minor alarm.	
Alarm In 1&2	Off – Alarm Input not configured	New for [redacted]
	Solid Green – Alam In configured, no alarm detected	
	Blinking Red – Major alarm detected	Same function and location on [redacted] SKUs
	Solid Red –Minor alarm detected	
Console	Off – RS232 Console via RJ45 connector selected	New for Camaro
	Solid Green – USB Console via mini-USB connector	Replaced by Express Setup on [redacted] skus
Ports	Off – no link	Same function and location on [redacted] SKUs
	Solid Green – Port link, no activity	
	Flashing Green/Off – Link healthy with activity	
	Alternating Green/Amber – Link Faulty/Error	
	Solid Amber – Port Disabled	
Express Setup	Off - Switch is configured as a managed switch.	Replaced by EIP Net Status LED on [redacted] skus [redacted]'s express setup
	Solid Green - Switch is in initial setup.	
	Blinking Green - Switch is in initial setup, in recovery, or initial setup is incomplete.	
	Solid Red - Switch failed to start initial setup or recovery because there is no available switch port to which to connect	

LED:	LED Definition:	Notes
	the management station. Disconnect a device from a switch port, and then press the Express Setup button.	LED moves to replace Console LED

2.2.4.6.1 [redacted] Specific LEDs

EtherNet/IP Mod Status LED: This LED replaces the System LED on the Cisco skus. A bi-colored LED that is red or green and flashing or steady on/off. This allows forsix unique states. This LED indicates information about the Module in conformance with the EtherNet/IPspecification from the ODVA. See table below for specific details. (This LED should have the same behavior as on the Stratix 8000.)

Indicator state	Summary	Requirement
Steady Off	No power	If no power is supplied to the device, the module status indicator shall be steady off.
Steady Green	Device operational	If the device is operating correctly, the module status indicator shall be steady green.
Flashing Green	Standby	If the device has not been configured, the module status indicator shall be flashing green.
Flashing Red	Minor fault	If the device has detected a recoverable minor fault, the module status indicator shall be flashing red. NOTE: An incorrect or inconsistent configuration would be considered a minor fault.
Steady Red	Major fault	If the device has detected a non-recoverable major fault, the module status indicator shall be steady red.
Flashing Green / Red	Self-test	While the device is performing its power up testing, the module status indicator shall be flashing green / red.

EtherNet/IP Net Status LED. This LED replaces the Express Setup LED on the Cisco skus. A bi-colored LED that is red or green and flashing or steady on/off. This allows forsix unique states. This LED indicates information about the Network in conformance with the EtherNet/IPspecification from the ODVA. See table below for specific details. (This LED should have the same behavior as on the [redacted] 8000.)

Indicator state	Summary	Requirement
Steady Off	Not powered, no IP address	If the device does not have an IP address (or is powered off), the network status indicator shall be steady off.
Flashing Green	No connections	If the device has no established connections, but has obtained an IP address, the network status indicator shall be flashing green.
Steady Green	Connected	If the device has at least one established connection (even to the Message Router), the network status indicator shall be steady green.
Flashing Red	Connection timeout	If one or more of the connections in which this device is the target has timed out, the network status indicator shall be flashing red. This shall be left only if all timed out connections are reestablished or if the device is reset.
Steady Red	Duplicate IP	If the device has detected that its IP address is already in use, the network status indicator shall be steady red.
Flashing Green / Red	Self-test	While the device is performing its power up testing, the network status indicator shall be flashing green / red.

Express Setup LED. The Express setup LED is in a different location on the Rockwell skus. Since the EIP Net LED replaces the Cisco Express Setup LED, the setup functionality is moved to replace the Console (USB) LED. The [redacted] SKUs will not have a console LED. The functionality will be the same as on the Cisco skus, but it will be on a different LED location.

2.2.4.7 Setup Button

All sku's provide a recessed Setup button to enable Express setup. The button is located on the front of the chassis. (Note that [redacted] SKU's don't have amode-button switch.)

2.2.4.8 SD Card

All sku's provide a removable SD flash card. The SD is hot swappable and front accessed. There is a cover which helps protect the SD Flash card, and holds the card firmly in place. The cover will be hinged and fasten closed with a captive srew. This will prevent the card from coming loose and protect against shock and vibration. The interface will support all SD and SDHC cards (which can go up to 32GB per the spec.

2.2.4.9 Fans

No moving parts (including fans) will be installed in any SKU.

2.3 Feature List (Software/Firmware)

All features/functionality and operation of IE2K/S7K switches are the same as that of IE3K, unless otherwise noted below. In addition, the IE2K/S7K implements the feature license (IA Lite and IA Base) with a single IOS image. Please refer to section 3.2 for a complete list of supported features in Camaro.

The following paragraphs describe enhanced and new features for the IE2K/S7K system.

2.3.1 Licensing Model

The IE2K/S7K implements the feature license (IA Lite and IA Base) with a single IOS image. For RA, IE2K/S7K, the customers can specifically order different SW packages via a unique

catalog item at [redacted] This information is integrated into the Cisco licensing model and shipped with the product from manufacturing.

For development and testing purposes (before and after FCS), [redacted] will have the ability to switch images (base vs. lite).

2.3.2 IOS Boot-up

[redacted] boot-up time will be targeted for less than 60 seconds. The optimization will involve in changing image compression algorithm, disabling memory test, system file checks and POST. A CLI will be provided to re-enable the above tests; but they will be disabled by default. Please note that there is always risk for not able to discover any HW failure when all system start-up tests are disabled.

2.3.3 Download Recovery

[redacted] NVRAM and SD card will be able to store at least two IOS images to handle an image download failure. [redacted] will ONLY operate on the Cisco SD flash card and reject all other commercial SD flash card. The SD flash card will be an orderable option and will ship with an IOS image.

2.3.4 OBFL

[redacted] will support On-Board Failure Logging (OBFL) which collects up-time, temperature. The collected data will be stored in a dedicated 2 MB flash memory. This feature has already been delivered on pixar/sharks and will be ported to [redacted] SKUs.

2.3.5 Link Diagnostics

[redacted] will provide an error rate as the percentage of the total line rate as an additional link diagnostics. Please refer to section 2.3.6 for Network Management (NM) support.

2.3.6 Network Management

[redacted] will support all NM currently supported on IE3K. Device Manager (DM) and Express Setup will be supported at FCS. Cisco Works and Cisco Network Assistant (CNA) will also be supported. The DM will be leveraged from the IE3K as the baseline for Camaro to provide the same graphical user interface (GUI).

PRD Section	Requirement	Eng Response
6.6.13.1		

NAT Monitoring & Troubleshooting	Ability to provide following monitoring and troubleshooting information: Current active translations (measure range: 90 sec) # of translated packets per unique translation entry (accumulated) # of total bypassed packets (accumulated) # of total dropped packets (accumulated) Above info should be available on per VLAN basis if the switch is performing translation per VLAN. These info need to be provided to CLI, DM, SNMP, CNA, CIP.	**Supported**
NAT Configuration	Provide clean and easy to understand configuration interfaces (CLI, DM GUI, CIP-AOP) to setup/modify/delete NAT configuration entries.	**Partial** – Need more design around incremental NAT assignment.
	(GUI only)Provide topology level hints to help end user understand what configuration need to happen on other related switches/routers to make NAT work	**Unsupported**
6.6.13.7		
Smartports	A new feature has been proposed for the [redacted] 8000 to allow [redacted] and customers to develop their own macros and connect those to the Device Manager and CIP environment (pull down menu). This should also be implemented in the S7000. The functionality exists currently in the CLI to add custom smartports. The custom configurable smartports in the CLI should be applicable via Device Manager and CIP.	**Supported - Will provide text box entry for custom macros.**
6.8.1.1		
Platform Support	1. Cisco IE 2K / [redacted] S7K entry level platform support. This includes	**Supported**

	the capability to select one or two power inputs via DM.	
TDR and Link Diagnostics (See 2.3.5)	2. The integrity of a media connection is a fundamental issue in the factory automation markets. The TDR and Link Diagnostics detection helps identify the media issues in a rugged environments. Thesetwo features need to be configurable and manageable (diagnostics) via DM and CIP tool. The purpose is to provide visibility to connections which may be marginal. TDR feature should be configurable via DM, similar to CLI and all the CLI diagnostics should be visible under the monitor tab in DM. For DM this should be a new tab under the "monitor" section. The user can run the TDR test by pushing a button upon entering the TDR tab. The results on a per port basis will be displayed as a visual chart or in a graphic format. Link Diagnostics will have a separate display in DM.	**Supported**
STP Configs	3. Expanded STP configurations in Device Manager – The IE2K/S7K should support MST, PVST and RPVST configurations and diagnostics (STP issues and changes) on the DM web based GUI. This is needed for compatibility issues with factory automation and plant floor IT devices. VW has requested the DM enhancements. This is for DM and CIP interface.	**Supported**
Enable/Disable Port Security	a. Ability to turn port security on and off on a port by port basis as a configuration selection in DM and CIP. ***The equivalent IOS CLI is 'switchport port-security' under interface configuration mode.***	**Supported**

Configure Devices	b. Ability to configure the number of devices enabled on the port via port security The maximum number of MAC addresses allowed in the port-security can be specified by the following IOS CLI: Switchport port-security maximum VALUE	**Supported**
Configure MACs	c. Ability to identify the MACIDs which are allowed per port when port security is turned on and the devices are learned. The functionality can be achieved by selecting the IOS port security modes and if the sticky mode is selected, the user should be able to see the MACID's via CIP/DM. The user interface should be designed to show dynamically learned MAC addresses on this interface when user gets into the port-security interface. Then the user has the option to select which MAC addresses are intended for sticky, i.e., keep in the IOS configuration file so they are not lost after switch reload. At this same interface, user can also manually enter a different MAC address as a statically configured MAC address to be accepted by IOS. The corresponding IOS CLI is *Switchport port-security mac-address sticky [MAC ADDRESS]* The CIP object to achieve similar functions is subject to coordinated design effort with [redacted] Add-on-profile developers.	**Supported**
Indicate security fault	d. Enhance CIP and DM interface to provide an indication when an unauthorized device is on a specific port. The indication will also include the offending MACID.	**Supported**

6.8.1.1		

2.3.7 MIB

[redacted] will support the MIBs currently supported on the IE3K. In addition, CISCO-NAT-EXT-MIB and CISCO-IETF-NAT-MIB will be leveraged to include NAT monitoring parameters listed in section 2.3.1.4.1. All support MIBs will be read-only.

2.3.8 Egress Storm Control

This feature will be met by allowing DM or CIP to configure the pre-existing IOS port shaper functionality. A new per-port CIP object will need to be added to support this configuration, but there will be no changes to the port shaper feature itself.

2.3.9 Network Address Translation (NAT)

This section briefly described NAT support for IE2K/S7K. The NAT configuration will be available via CLI, CIP interface support for Add-On-Profile (AOP). Please note that the AOP program is owned by Rockwell. The IOS will provide the CIP interface support for the configuration. Please see section 2.3.6 for network management support.

IE2K/S7K NAT functionality will ONLY be available on active uplink port(s). It will be static NAT, (mapping an unregistered IP address to a registered IP address on a one-to-one basis) for unicast IPv4 traffic. NAT will be performed on per VLAN basis, maximum of 128 VLANs. The system will support a maximum of 128 translations. The following table summarizes the IE2K NAT requirements.

Category	Req#	Requirement	Description
NAT Function	NAT1.1	1:1 Static NAT	One to one translation of source IP address to another IP for unicast traffic coming from and to "inside" network.
	NAT1.2	Bi-directional	Ability to correctly translate the return traffic Ability to perform translation so that traffic originated from outside targeting at the external IP address can successfully reach the corresponding host on inside network.
	NAT1.3	Exceptions	Ability to bypass or drop the unicast

IRL	a. Add Ingress rate limiting to Device Manager similar to feature as it exists in CIP today (see figure below).	**Supported**
ERL	b. Add Egress rate limiting feature to the Device Manager and CIP. The objective is to limit the traffic to end devices which have specific performance constraints. Rate limits are typically represented by total packets per second. A User friendly mechanism for entering this limit per port is required.	**Supported**
Display logs / SNMP	6. Enhanced diagnostics on Device Manager – Configure and display SNMP traps and syslog configuration and diagnostic functions in the device manager.	**Partial - REDUCED FUNCTIONALITY**: Not possible to show all traps / logs. Will show as available to DM from IOS.
R/O mode	7. View only mode in Device Manager – Allow the ability to enter Device Manager in a read only mode without the need to enter a password. This would allow a user to view the Device Manager status and diagnostic information without the need for a password. Today you must enter a password to view the Device Manager status pages. If this implementation is not possible then add an additional read only password to Device Manager to allow someone the capability to view Device Manager displays only when this password is entered. The read only password would not allow you to make configuration changes. Upon integration the read only password would come with a default password already entered. It would not be necessary to change this password unless the user chose to.	**Unsupported**
new feature requests under	create new page in DM for new "link diagnostics"	**Supported**

			IP traffic that is not configured to be translated Central configuration needed to indicate if bypass or drop behavior is desired for unicast IP traffic Default option is drop for IE2K Ability to bypass non-IP traffic Ability to bypass/drop multicast, IGMP
	NAT1.4	Protocols fixup	Make sure following protocols will work properly with NAT: HTTP/HTTPS Profinet IO (unicast) PTP unicast (IEEE1588v2) ICMP ARP SNMPv1, v2 (RFC 2962, basic) Telnet SSH User should be able to choose which protocol to fixup. The default configuration will fixup ICMP, ARP, and Profinet IO.
Scalability	NAT2.1	Machine level switch (IE2K)	128 max unique entries per switch Max 128 VLAN (user specify , default to VLAN1) is allowed to have NAT configuration. No limitation on how many translation entries per VLAN (only constrained by the max entries per switch) When used in ring topology, each uplink need to be able to handle the above scalability requirement. Ability to define one or two (when used in ring) uplinks
Performance	NAT3.1	Wirespeed translation	Ability to translate at wirespeed control and management traffic (<5 micro second delay) Wirespeed translations is highly desirable for complex control

			applications Translation jitter between first entry and last entry in the table should be <30 micro seconds. Per flow translation jitter should be <20 micro seconds.
Manageability	NAT4.1	Monitoring & Troubleshooting	Ability to provide following monitoring and troubleshooting information: • Current active translations (measure range: 90 sec) • # of translated packets per unique translation entry (accumulated) • # of total bypassed packets (accumulated) • # of total dropped packets (accumulated) • Above info should be available on per VLAN basis if the switch is performing translation per VLAN. These info need to be provided to CLI, SNMP, CIP. Please refer to section 2.3.6 for Device Manager.
	NAT4.2	Configuration	Provide clean and easy to understand configuration interfaces (CLI, CIP) to setup/modify/delete NAT configuration entries. The configuration input can be single entries or IP address ranges. (GUI only) Provide topology level hints to help end user understand what configuration need to happen on other related switches/routers to make NAT work. Please refer to section 2.3.6 for Device Manager.
	NAT4.3	SNMP support	SNMP MIB support for monitoring parameters
	NAT4.4	CIP support	Common Industrial Protocol support for the NAT feature configuration and monitoring/troubleshooting Configuration:

			Create NAT entries with VLAN association Modify/Delete entries Choose bypass/drop mode Monitoring: Defined in Req. 4.1
	NAT4.5	DM support	Refer to section 2.3.6

2.3.10 CIP

[redacted] will support all CIP functionality currently supported on the IE3K. In addition, CIP will be enhanced to support the following features' configuration and diagnostics via Rockwell management tool. All new CIP objects to achieve these enhancements are subject to coordinated design effort with [redacted].

2.3.10.1 STP and MSTP

Camaro will provide the ability to configure and display diagnostics for PVST+, RPVST+, and MSTP.

2.3.10.2 Enhanced Port Security

[redacted] will provide the ability to configure and display information with regards to the enhanced port security. The feature will include:

a. Turn port security ON/OFF on a port by port basis
b. Configure number of devices enabled on the port via port security
c. Ability to display MAC ids which are allowed per port when port security is enabled and devices are learned. This functionality is achieved by selecting the IOS sticky mode.
d. Provide an indication including the offending MAC id when an unauthorized device is on a specific port.

2.3.10.3 VLAN Enhancement

Camaro will provide the ability to create/remove VLAN from the switch.

2.3.10.4 Egress Storm Control

Camaro will provide the ability to configure/display diagnostics for this feature specified in section 2.3.8.

2.3.10.5 Link Diagnostics

Camaro will provide the ability to configure and manage TDR including the cable diagnostics enhancement as described in section 2.3.5

2.3.10.6 CIP Password encryption for displaying configuration

This feature will encrypt the CIP password which is saved in the switch config.

2.3.10.7 NAT

This feature will provide NAT monitoring parameters as listed in NAT requirements. The new CIP object(s) to achieve this enhancement is subject to coordinated design effort with [redacted].

2.3.10.8 Configurable Controller Idle and Fault actions

Two independent states are defined in this feature.

1. Controller Idle state – defined as CIP I/O connection idle state
2. I/O connection fault – defined as CIP I/O connection timed out.

Currently, in the IE3K, when the controller indicates that it is in "idle" state, the switch basically does nothing. Effectively, the switch holds all ports in their last states. With this feature, [redacted] will provide the capability to configure (during the startup configuration stage via CIP objects) two lists of actions associated with each of the state: "controller's idle state" or the "I/O connections fault". These parameters are saved in the configuration. The following are the configurable actions for either event:

- Do nothing (leave ports in their current state)
- Turn on/off all ports
- Turn on/off specific ports

2.3.11 Smartports Templates

This feature will be leveraged from IE3K using 12.2(58)SE as the baseline to provide easy connectivity for individual Industrial Ethernet applications. In addition to the current supported templates, the IE2K will also add the following function:

a. Allow "new created custom configurable smartports" via CIP. Please see section 2.3.13 for more information on custom configurable smartports.

Due to the licensing feature, some smartports templates will be modified for the IE Lite version.

Please refer to section 2.3.6 for NM support.

2.3.12 IEEE 1588v2 (Precision Time Protocol)

[redacted] will support the IEEE 1588 v2 functionality currently supported on the IE3K. The packet performance and operational default will be the same as IE3K. In addition, an

enhancement will be made to avoid timestamp collision as describe in the customer issue (CSCtl09690).

2.3.13 Configurable Smartports

[redacted] will provide the capability to create custom configurable smartports macro via CLI. There will be NO anti-macro created for the new custom smartport. The user can delete a macro-applied configuration on an interface by entering the "default interface" interface configuration command. The new custom smartport macro will be available for CIP and DM. Please refer to section for 2.3.6 for NM support.

2.3.14 Removable SD Flash Card

[redacted] will support the removable SD flash card in PC readable format. During the system reload, the system will boot from either on-board flash or SD flash card depending on the following conditions:

a. presence of SD card
b. and SD's boot parameters

If the SD card is present, the switch will boot from the SD flash with its configuration. If the SD card is not present, the switch wll read the on-board boot parameters and boot from the specified IOS image on the on-board flash. The SD flash card will NOT automatically override the on-board flash with its IOS image and configuration. To sync the image in either direction, the user has to initiate a sync (or copy) command to establish the transaction via CLI, DM, or CIP. Upon a "write" command, the switch will save the config onto the media from which it booted. Please refer to section 2.3.6 for NM support.

Please note that the switch will ONLY operate on the Cisco SD flash card and reject all other commercial SD flash card. The SD flash card will be an orderable option and will ship an IOS image.

2.3.15 Alarm Input/Output

[redacted] will provide CLI to configure whether or not the alarm relay is normally energized. By default, the configuration will have the relay normally de-energized. The behavior is described in the following table.

Alarm State	Alarm Mode	Form C Alarm Relay Contact State	Comment

	(Polarity)	N.O. Contact	N.C. Contact	
Power is off	N/A	Open	Closed	This is the de-energized state of the form-C alarm relay
No Alarm event is detected, or initial power-on setting	Normally De-energized	Open	Closed	With relay mode set to Normally De-energized, the relay remains de-energized in the absence of a defined alarm event
	Normally Energized	Closed	Open	With relay mode set to Normally Energized, the relay remains energized in the absence of a defined alarm event.
One or more Alarm events are detected	Normally De-energized	Closed	Open	With relay mode set to Normally De-energized, the relay is energized when a defined alarm event is present
	Normally Energized	Open	Closed	With relay mode set to Normally Energized, the relay is de-energized when a defined alarm event is present.

2.4 Features Not Addressed

2.4.1 HW

N/A

2.4.2 SW

The following functionalities will NOT be addressed in this project:

- IE3K NAT functionality is NOT addressed in this project
- NAT Requirement 1.5 which include the following protocols: FTP, SIP, Skinny, TFTP
- NAT configuration via CNA (indicated in PRD as Priority 2)
- The IOS boot-up time will not meet the highly desirable goal of 30 seconds. The anticipated boot-up time currently with fast boot enabled is < 60 seconds.
- The egress storm control (egress rate limiting) feature will not be implemented due to HW limitation. However, an alternative solution (egress port shaping) is provided which meet the high-level goal of the requested feature.

2.5 Software Impact Assessment

The following items mayimpact another team's uptake of the NAT feature for future programs:

- Modifications to existing MIB(s)
- There are specific HW resource requirementsrequired to implement NATthat must be implemented in any future program (e.g. FPGA, Memory/CPU)

The following items may impact another team's uptake of the OBFL feature for future programs:

- Flash partition for OBFL
- There are specific HW resource requirementsneeded to implement OBFL such as HW temperature sensor

2.6 Testability Considerations

The CPU PCBA will have the standard edge fingers to support the SAM connector. This will allow for Yeti-3 CPU program trace and debug, and will also provide access to program the Sparkplug FPGA. Each PCBA will have JTAG devices chained together for test point reduction ease of debugging. The Stretch PCB will add debug header for Jeeves FPGA programming and debug.

2.7 Manufacturing Consideration

2.7.1 Legal

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment
LEGAL1B	Must meet EU Rohs 6 (Pb-free) requirements	Required	Global	Req't will be met
LEGAL2	Must meet China Rohs requirements (labeling, documentation, packaging)	Required	Global	Req't will be met

LEGAL14	If 3rd party IP is being purchased, a SW License agreement must be approved (which involves engagement with GCM and Cisco legal) before a purchase order can be issued to the supplier. These agreements can take weeks to months to negotiate depending on the other parties' willingness to agree to Cisco's terms and conditions that are in the SW License Agreement. it is much easier to use IP of which we (Cisco) have already purchased and negotiated a SW License Agreement for.	Required	Global	N/A. No 3rd party IP is being purchased on Camaro.

2.7.2 Brand Protection

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment
BRANDPROT1	Product must adhere to Counterfeit Prevention Cisco Manufactured Certificate Request Requirements (EDCS-458731)	Required	Global	Req't will be met
BRANDPROT2	Product must adhere to requirements identified in Brand(Counterfeit) Protection (EDCS-460345)	Required	Global	Req't will be met
BRANDPROT7	Use new Cisco Logo on external packaging	Optional	Global	Req't will be met

2.7.3 Electrical

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment
ELECTRICAL1	Cisco Producibility Guidelines (EDCS-7002900)	Required	Global	Req't will be met
ELECTRICAL2	Optics Producilbility Guidelines (EDCS-156122)	Required	Global	Req't will be met
ELECTRICAL4	Generic IDPROM (ENG-14099).	Required	Global	Reqt will be met
ELECTRICAL8	PCB Supplier Technology Matrix (EDCS-361471)	Required	Global	Req't will be met
ELECTRICAL10	Product design shall comply with UDI Specifications (EDCS-231946) MECHANCIAL103	Required	Global	Req't will be met
ELECTRICAL13	CAD PCB Manufacturing Output Package Definition (EDCS-514791)	Required	Global	Req't will be met

ELECTRICAL25	Use RoHS 6 Compliant components where approved (refer to LEGAL1B requirement)	Required	Global	Req't will be met
ELECTRICAL55	Must meet Cisco Pb-Free Qualification Specificiations identified in EDCS-281405 for components	Required	Global	Req't will be met
ELECTRICAL56	Product must adhere to EDCS-156122 Optics Producibility Guidelines PRDSPECIFIC1	Required	Global	Req't will be met
ELECTRICAL57	Optics must meet Cisco Pb free requirements identified in EDCS-491485 PRDSPECIFIC7	Required	Global	Req't will be met
ELECTRICAL58	Requirement Detailed Description – No Reliability Grade (RG) or L2 Use Condition (UC) mismatch exists that raises a gating error. If a gating error (or errors) exist, issue has been escalated and resolved (components have been replaced; or, Prod Ops and BU HW engr directors have signed off). (EDCS-873251 - Segmented AVL-CQR Implementation Guide)	Required	Global	Req't will be met

2.7.4 Mechanical

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment
MECHANICAL1	[Std] Product design shall comply with Design for Manufacturability/Assebmly Guidelines (EDCS-7021930). ELECTRICAL5	Required	Global	Req't will be met
MECHANICAL2	Component Mechanical Design Best Practices (EDCS-423906)	Required	Global	Req't will be met
MECHANICAL3	Cisco Heatsink Assy Procedure (EDCS-703204-0000)	Required	Global	Req't will be met
MECHANICAL4	Sheetmetal Tolerance Specification (95-0735-01)	Required	Global	Req't will be met
MECHANICAL16	Use RoHS 6 Compliant components where approved	Required	Global	Req't will be met
MECHANICAL17	Product design shall comply with Cosmetic Specifications (Reference Procedure 95-2733-01)	Required	Global	Req't will be met
MECHANICAL22	Leverage use of common mechanical parts across platforms (fans, PS, chassis, etc)	Required	Global	Req't will be met
MECHANICAL23	Use standard EMI clips and hardware	Required	Global	Req't will be met
MECHANICAL86	Product design shall comply with recommended Heat Sink Attach Materials EDCS-202698	Required	Global	Req't will be met

MECHANICAL92	[Std] Design should follow Mechanical DFM Process for New Product Introduction (EDCS-575428)	Required	Global	Req't will be met
PRDSPECIFIC4	Product must adhere to Cleaning and Inspection Procedure for Fiber Optics Connectors (703683-0000)	Required	Global	Req't will be met

2.7.5 Packaging

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment
PACKAGING1	Must meet Package Test Specificiations EDCS-7002970	Required	Global	Req't will be met
PACKAGING2	Chassis and all spares (FRUs) must be designed to have strength and durability to pass MDVT non-operational shock and vibration requirements as specified in ENG 3396.	Required	Global	Req't will be met
PACKAGING4	Chassis must not have protrusions. Exceptions will require special and expensive packaging solutions. Validate in Cost roll-up.	Required	Global	Req't will be met
PACKAGING5	Need sufficient bearing area on all 6 faces of the chassis	Required	Global	Req't will be met
PACKAGING7	Complete FAI per requirements	Required	Global	Req't will be met
PACKAGING9	Product packaging should follow the Cisco Packaging & Shipping Standard (EDCS-7011020) Packaging must be designed to fit efficiently on shipping pallets.	Required	Global	Req't will be met
PACKAGING10	Packaging design must consider Direct Fulfilment (DF) strategy. Optimize to preserve quality as the unit passes though DF, and optimize for low cost for material handling at DF.	Required	Global	Req't will be met
PACKAGING11	Use standard packaging that is capable of supporting multiple platforms.	Required	Global	Req't will be met
PACKAGING12	Must design in 100% recyclable packaging materials (intermediate and final product)	Required	Global	Req't will be met
PACKAGING13	MDVT must use fixtures based on packaging design team input	Required	Global	Req't will be met
PACKAGING14	The palletization of product by the supplier must follow the Palletization Requirements (EDCS-7036530)	Required	Global	Req't will be met

PACKAGING16	Multipack packaging must be considered as a packaging option for the product and developed in parallel with the single-pack packaging (EDCS-724668). Reference website http://wwwin.cisco.com/mfg/organizations/mo/moe/multipack/	Required	Global	Req't will be met

2.7.6 Mfg Test

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment
MFGTEST1	Structural test (ICT) must have 98% or greater coverage	Required	Global	Goal will be to have ≥ 98% coverage
MFGTEST2	No manufacturing impacting Software bugs	Required	Global	Req't will be met
MFGTEST4	Boards must meet PCB Design for Test (EDCS-7004080)	Required	Global	Req't will be met
MFGTEST5	ASICs must meet Cisco ASIC DFT Metrics - DFT Requirements (EDCS-250999)	Required	Global	Req't will be met
MFGTEST9	Diagnostics should meet Manufacturing Diagnostics Requirements (EDCS-649798)	Required	Global	Req't will be met
MFGTEST10	Diagnostic coverage should be at least 98% of all functional logic and it must be thoroughly tested during EDVT before release to production	Required	Global	Goal will be to have ≥ 98% coverage
MFGTEST12	All plug-in modules shall be identifiable and controllable through both diagnostics and IOS.	Required	Global	Req't will be met
MFGTEST14	Diagnostic software should provide read-write utilities for the EEPROM.	Required	Global	Req't will be met
MFGTEST22	Must follow Diagnostics Requirement EDCS-75589. The card must support 2 corner board level tests in manufacturing for voltage margining across every card type. Software controllable voltage margining on all power rails simultaneously. Individual rails do not need to be independently controlled for manufacturing 2Corner process requirements.	Required	Global	Req't will be met
MFGTEST25	Must define product specific diagnostic requirements by Execution Commit.	Required	Global	Req't will be met by FCS.

2.7.7 Commodity & Comm Risk

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment

COMMODITY5	All ASICs must follow RFQ process (as specified in section 3.6 of ASIC Design Process Overview (EDCS-346254) and ASIC Sourcing Process (EDCS-570459); as well assupport the ASIC Strategy.	Required	Global	Req't will be met
COMMODITY6	All PCB, Flash, SRAM, DRAM, Optics, CAM, Interconnects, Standard Products, External Pwr Adapter, Fans/Fan Trays, Board Mounted Power supply and LCD shall have at minimum two suppliers approved by GSM via the RFQ awards process. High volume components as defined by sourcing strategy shall have minimum 3 suppliers. COMMODITY 31,35,39,43,46,55,61,67,73,78,83	Required	Global	Some components will be sole sourced. Goal will be to get multiple suppliers when available.
COMMODITY7	All single source commodities such as ASIC, PLD, MMC-MPU, MMC-Datacom and enclosures shall follow RFQ awards process.	Required	Global	Req't will be met
COMMODITY8	The Risk Factor 1 parts in the BOM must contain risk mitigation plans ELECTRICAL17	Required	Global	Req't will be met
COMMODITY9	Product must obtain 100% PSL compliance ELECTRICAL19	Required	Global	Req't will be met
COMMODITY11	Requirement: All prototype builds are required to be processed at a qualified production site, unless otherwise approved by the Sourcing Commodity Manager. Recommend 10 day turn + 2 day ship at qualified production sites for best cost. Include BU specific sourcing charts from GCM website PCB strategy links.	Required	Global	Req't will be met
COMMODITY13	If 3rd party IP is being purchased, a SW License agreement must be approved (which involves engagement with GCM & Cisco legal) before a purchase order can be issued to the supplier. These agreements can take weeks to months to negotiate depending on the other parties' willingness to agree to Cisco's terms and conditions that are in the SW License Agreement. Needless to say, it is much easier to use IP of which we/Cisco have already purchased and negotiated a SW License Agreement for.	Required	Global	N/A. No 3rd party IP is being purchased on Camaro
COMMODITY14	Requirement that the PCB design utilize approved material. If new material is required, contact Sourcing Commodity Manager. Include Master Material List EDCS link.	Required	Global	Req't will be met

COMMODITY15	Contact the Sourcing Commodity Manager for predictive cost. Utilizing the costing model and previous pricing history for specific attributes, a predictive price range will be provided.	Required	Global	Req't will be met
COMMODITY16	PCB should be multi sourced.	Required	Global	Req't will be met
COMMODITY17	Requirement that the PCB design utilize suppliers recommended specific to the BU. If new technology is required that the current supply base does not provide, contact Sourcing Commodity Manager. Include BU specific sourcing charts from GCM website PCB strategy links.	Required	Global	Req't will be met
COMMODITY18	Requirement that the PCB be designed to the lowest technology level possible. Include Tech Attribute Matrix EDCS link.	Required	Global	Req't will be met
COMMODITY21	Design Preferred Suppliers. Example Xilinx, Altera	Required	Global	Req't will be met
COMMODITY23	All commodities, MMC-MPU, SRAM, DRAM, Flash, CAM, Standard Products should be sourced per Commodity Strategy as defined by GSM. COMMODITY 26,29,33,37,41,55	Required	Global	Req't will be met
COMMODITY48	Use Interconnect PSL suppliers for all applications regardless of power, ground or signal requirements. In cases where proprietary technologies are considered, design licensing is to be pursued at design concept phase. Contact GSM Sourcing Commodity Manager.	Required	Global	Req't will be met
COMMODITY53	Requirement that part re-use (Risk Rated 2 parts) should be considered before pulling a brand new parts.	Required	Global	Req't will be met
COMMODITY63	Requirement - Isolated Std. Product - 2 sources at low volume (<10k per year) & 3 sources at medium- high volume (10k - >100k per year)	Required	Global	Some components will be sole sourced. Goal will be to get multiple suppliers when available
COMMRISK1	The BOM must not contain Risk Factor X parts at the time of FCS ELECTRICAL16	Required	Global	Req't will be met
COMMRISK3	All RR-1A parts must have at least one qualified and one in Process Qual (IPQ) second sources at FCS.	Required	Global	Req't will be met for most components. There will be some components (such as

				ASIC & Phy) that will be sole sourced.

2.7.8 Supply Chain

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment
SUPPLYCHAIN1	All supply chain checklist items should be identified by CC to ensure proper supply chain design. The accompanying process document (EDCS-630746) is also available for further detail.	Required	Global	Req't will be met
SUPPLYCHAIN3	If TAA compliance is required by Marketing/Sales, then the Supply chain must be designed to meet those requirements for the portion of sales that are projected to go to the U.S. government. (build in TAA approved country)	Required	Global	Req't will be met
SUPPLYCHAIN5	Must design the product Supply Chain, so that it can be built by all of Cisco's perfered CMs. The CM will be choosen with total land cost in mind, as well as balance within the CMs, and BU alignment.	Required	Global	Req't will be met

2.7.9 Quality

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment
QUALITY10	Product must adhere to Reliability Demo. Test (RDT) EDCS-7005770	Required	Global	Req't will be met
QUALITY11	MTBF calculation must meet or exceed MTBF target at Gate Review (CC & Final TRR)	Required	Global	Req't will be met

2.8 Network Management Considerations

[redacted] will support all NM currently supported on IE3K. Cisco Works will also be supported at FCS in addition to Device Manager (DM), Cisco Network Assistant (CNA), and Express Setup. See Section 2.3.6 for details.

2.9 Patentability Considerations

Throughout the [redacted] program we will identify any aspects of the system that may be patentable. Patent ideas will be discussed and executed through the standard Cisco process during the program.

2.10 Brand (Counterfeit) Protection Considerations

[redacted] complies with EDCS-460345 for Brand Protection Guidelines. [redacted] will use a smart-chip based approach using the Quack2 plus security chip (15-10898-01) for the counterfeit protection. Quack2 is the next generation encryption ASIC used to verify the authenticity of the platform by storing private keys. It is used only to maintain the Universal Device Identifier(UDI) which is used by the platform. It provides digital signature and SW authentication at boot-up. It is similar to the Quack chip used on previous products, except its interface to the CPU is I2C instead of UART. Quack2 is connected to Yeti-3 via the 4-port I2C MUX.

3 External Specifications

Most of the L2 software functionality of [redacted] switches are the same as IE3k switches. In addition, the [redacted] software will support removable SD flash card and NAT. Please refer to section 3.2 for the complete feature list supported in [redacted] switches.

3.1 Overview

[redacted] switches will be managed through one of the following methods:

- Using CLI interface over serial connection to the switch console or over a telnet session
- Using the web management interface through a browser (Network Management)
- Industrial management tools via CIP/Profinet
- Using the Network Management Application via SNMP

The CLI interface supports the standard IOS commands. Please see section 2.3.6 for Network Management support.

3.2 Functional Requirements

3.2.1 IOS features

The following table lists IOS supported features for these two software versions, Industrial Automation (IA) Lite and IA Base.

Switch Specifications	IA Lite (Layer 2 Lite)	IA BASE (Layer 2)
VLANs supported	64	255
4096 VLAN IDs	Yes	Yes
Number of STP Instances	64	128
MAC Addresses	8K	8K
64 Bit Counter on Gig Ports	Yes	Yes
Maximum EtherChannel Groups	No	6
Number of Ingress Queues	No	2
Number of Egress Queues	No	4
Number of Ingress Policers per Port	No	64 FE,
	No	64 GE
Layer 2 Features	**IA Lite (Layer 2 Lite)**	**IA BASE (Layer 2)**
802.3	Yes	Yes
802.3u (FE)	Yes	Yes
802.3x (Flow Control)	Yes	Yes
802.3ad (LACP)	Yes	Yes
802.3z (CWDM)	Yes	Yes (Gig only)
802.1p	Yes	Yes
802.1q	Yes	Yes
802.1d (spanning-tree)	Yes	Yes
802.1s (MSTP)	Yes	Yes
802.1w (RSTP)	Yes	Yes
STP Syslog Messages	Yes	Yes
Flex Link/ Backup Interface	No	Yes
Flex Link/ Mac Move Notification (MMN)	No	Yes
Flex Link Pre-emption	No	Yes
Flex Link VLAN Load Balancing	No	Yes
Flex Link - Multicast fast convergence with flexlink failover	No	Yes
Resilient Ethernet Protocol (REP)	Yes	Yes
REP Enhancement - Clear REP Counters via CLI	Yes	Yes
REP Enhancement - LSL Age-out Timer 3-10 sec, .5 sec inc.	Yes	Yes
REP Enhancement - Hot Ice Support (for Config Rollback)	Yes	Yes
REP Enhancement - REP Edge No Neighbor	Yes	Yes
REP Enhancement - Multicast Performance with MVR and IGMP Snooping (<200ms convergence with 200 VLANs)	Yes	Yes
Trunk Failover (Link State Tracking)	No	Yes
STP PortFast	Yes	Yes
STP PortFast on Uplink Ports	Yes	Yes
STP UplinkFast	Yes	Yes
STP BackboneFast	Yes	Yes
Clustering	Yes	Yes
Fast EtherChannel	No	Yes
Gigabit EtherChannel	No	Yes
PAgP	No	Yes
Enhanced PAgP for VSS	No	Yes
ISL Trunking	No	No
802.1Q VLAN Trunking	Yes	Yes

Multicast EtherChannel Load Balancing	No	Yes
VLAN (voice) aware port security	Yes	Yes
IP Phone detection enhancement	Yes	Yes
VTPv2	Yes	Yes
VTP (VLAN Trunking Protocol) - Server, Client, Transparent Modes	Yes	Yes
VTP Pruning	Yes	Yes
DTP (Dynamic Trunking Protocol)	Yes	Yes
PVST	Yes	Yes
PVST+	Yes	Yes
Rapid PVST+	Yes	Yes
UDLD	Yes	Yes
Aggressive UDLD	Yes	Yes
Mini-jumbo Frame Support	Yes	Yes
Jumbo Frames	Yes (Gig only)	Yes (Gig only)
Forced 10/100 Auto Negotiation	Yes	Yes
Voice VLAN	Yes	Yes
Per port enabling/disabling of unknown unicast/ multicast flooding	Yes	Yes
IP Host connectivity such as telnet, DHCP, BootP Client, DNS	Yes	Yes
Static MAC Addressing	Yes	Yes
Dynamic MAC Addressing	Yes	Yes
Dynamic Access Ports (Dynamic VLAN)	Yes	Yes
Port duplex/speed	Yes	Yes
Port Flow Control	Yes	Yes
User configurable management VLAN	Yes	Yes
SysLog	Yes	Yes
VTP v3	No	Yes
IPv6	**IA Lite (Layer 2 Lite)**	**IA BASE (Layer 2)**
Hardware capable of supporting IPv6	Yes	Yes
IPv6 MLDv1 and v2 Snooping	No	Yes
IPv6 Host support (- IPv6 support: Addressing; IPv6: Option processing, Fragmentation, ICMPv6, TCP/UDP over IPv6; Applications: Ping/Traceroute/VTY/SSH/TFTP, SNMP for IPv6 objects)	No	Yes
HTTP, HTTP(s) over IPv6	No	Yes
SNMP over IPv6	No	Yes
SysLog over IPv6	No	Yes
IPv6 Stateless Auto Config	No	Yes
DHCP based Auto Config (Auto Install) and Image download	Yes	Yes
IPv6 Neighbor Discovery Throttingly	No	No
IPv6 QOS Trust	No	No
Security	**IA Lite (Layer 2 Lite)**	**IA BASE (Layer 2)**
Static Access Ports	Yes	Yes
Port Security	No	Yes
Port Security MAC Aging	No	Yes
Port Security for Voice VLANs	No	Yes
Trunk Port Security	No	Yes
MAC address notification	Yes	Yes

Multilevel Console Security	Yes	Yes
Secure Copy Protocol (SCP)	Yes	Yes
Private VLAN Edge (Protected Port)	Yes	Yes
802.1 x	No	Yes
802.1x with VVID/PVID	No	Yes
802.1x with VLAN assignment	No	Yes
802.1x Guest VLAN	No	Yes
802.1x guest vlan consistency	No	Yes
802.1x with WOL (Wake on LAN) support	No	Yes
802.1x Auth-Fail-VLAN	No	Yes
802.1x Inaccessible authentication bypass	No	Yes
802.1x Auth-Fail -Open	No	Yes
802.1x MAC-Auth-Bypass	No	Yes
802.1x with ACLs	No	Yes
802.1x w/Port Security	No	Yes
802.1x Radius Accounting	No	Yes
802.1x MIBs	No	Yes
802.1x voice aware, MAB security violations	No	Yes
802.1x Readiness check	No	Yes
802.1x Supplicant with NEAT (access switch authentication with aggregation switch for physical security)	No	Yes
Secure Shell SSHv 1.5	No	Yes
Secure Shell SSH 2 Server	No	Yes
Generic Message Authentication for SSH Protocol - RFC 4256	No	Yes
HTTP(S)	No	Yes
SSL	No	Yes
Unicast MAC Filtering	Yes	Yes
TACACS+	Yes	Yes
Local RADIUS Server	Yes	Yes
RADIUS Client	Yes	Yes
RADIUS Server Load Balancing	No	Yes
SNMPv3 crypto (3DES and AES)	No	Yes
BPDU Guard	Yes	Yes
BPDU Filtering	Yes	Yes
Loopguard	Yes	Yes
Spanning Tree Root Guard (STRG)	Yes	Yes
SPAN	Yes	Yes
DHCP Snooping	Yes	Yes
Dynamic ARP Inspection	No	Yes
IP Source Guard	No	Yes
Unicast/Multicast/Broadcast Storm Control	No	Yes
Packet Based Storm Control	No	Yes
Time-based ACLs	No	Yes
DSCP-based ACLs	No	Yes
PACLs	No	Yes
VLAN 1 Minimization	Yes	Yes
NAC-L2 IEEE 802.1x	No	Yes
Voice aware - 802.1x and MAB security violations	No	Yes
802.1X Readiness Check	No	Yes
Flexible Authentication - for 802.1x, MAC Auth and Web Auth	No	Yes
802.1X switch supplicant with NEAT	No	Yes

802.1X with Open Access	No	Yes
802.1X, MAC Auth Bypass and Web auth with downloadable ACLs (dACL)	No	Yes
CDP enhancement for second port disconnect	No	Yes
Common Session ID for 802.1X and MAB	No	Yes
Authentication Framework Manager MIB	No	Yes
Conditional logging (interface based) for 802.1X and MAB	No	Yes
802.1X with Multiple Authentication (Multi-auth)	No	Yes
RADIUS Server load balaning	No	Yes
MAC move	No	Yes
RADIUS change of authorization	No	Yes
IEEE 802.1x User Distribution	No	Yes
Critical VLAN with multi-auth	No	Yes
CISCO-ADMISSION-POLICY-MIB support	No	Yes
Customizable web authentication	No	Yes
3DES and AES support with SNMPv3	No	Yes
IP source guard for static hosts	No	Yes
DHCP snooping ASCII circuit ID	Yes	Yes
Common session ID syslog Integration	No	Yes
802.1X with Multiple Authentication (Multi-auth)	No	Yes
3DES and AES support with SNMPv3	No	Yes
Quality of Service	**IA Lite (Layer 2 Lite)**	**IA BASE (Layer 2)**
Ingress Policing	No	Yes
Ingress Rate Limiting	No	Yes
Egress Bandwidth Limiting/port shaping	No	Yes
Number of Egress Policers per Port	No	Shaping
802.1p Priority	No	Yes
Ingress/Egress Strict Priority Queuing (Expedite)	No	Yes
Shaped Round Robin (SRR)	No	Yes
Weighted Tail Dop (WTD)	No	Yes
Storm Control - Unicast, Multicast, Broadcast	No	Yes
Packet Based Storm Control	No	Yes
Egress Shaped Queues	No	Yes
Ingress/egress Shared Queues	No	Yes
DSCP Mapping	No	Yes
DSCP Filtering	No	Yes
AutoQoS - VoIP	No	Yes
AutoQoS - VoIP Enhancement	No	Yes
Auto QoS 1.5	No	Yes
Trust Boundary Configuration	No	Yes
Global QoS (enable QoS)	No	Yes
Multicast	**IA Lite (Layer 2 Lite)**	**IA BASE (Layer 2)**
IGMP v1, v2 Snooping	Yes	Yes
IGMP v3 Snooping	Yes	Yes
IGMP v1, v2 Filtering	Yes	Yes
IGMP Snooping Timer	Yes	Yes
DHCP-Snooping-MIB	Yes	Yes
IGMP Throttling	Yes	Yes
IGMP Querier	Yes	Yes
Configurable IGMP Leave Timer	Yes	Yes

MVR (Multicast VLAN Registration)	No	Yes
Manageability	**IA Lite (Layer 2 Lite)**	**IA BASE (Layer 2)**
802.1x MIBs	No	Yes
PAE (Port Access Entity) MIB	No	Yes
NAC-NAD MIB Support and PAE MIB (New OID's Added)	No	Yes
Cisco-Port-QoS-MIB	Yes	Yes
Cisco-Port-Security-MIB	Yes	Yes
Cisco-DHCP-Snooping-MIB	Yes	Yes
Cisco-UDLDP-MIB	Yes	Yes
CISCO-ERR-DISABLE MIB	Yes	Yes
CISCO-CABLE-DIAG MIB	Yes	Yes
DHCP AutoInstall with a Saved Configuration	Yes	Yes
Express Setup	Yes	Yes
Device Manager	Yes	Yes
CMS	Yes	Yes
Cisco Network Assistant compatibility	Yes	Yes
Cisco Works compatibility	Yes	Yes
SPAN	Yes	Yes
Number of SPAN Sessions	1	2
SPAN for intrusion detection	No	Yes
RSPAN	No	Yes
Auto Configuration	Yes	Yes
Auto QoS (Voice)	No	Yes
Crash File	Yes	Yes
CDP v1, v2	Yes	Yes
LLDP-MED 802.1ab	Yes	Yes
LLDP-MED Location 802.1ab	No	Yes
LLDP_MED integration for CoS/DSCP	No	Yes
LLDP MIB	Yes	Yes
SNMP v1, v2	Yes	Yes
SNMPv3 non-crypto	No	Yes
SNMPv3 crypto	No	Yes
L2 Trace Route	Yes	Yes
Auto-MDIX	Yes	Yes
CLI	Yes	Yes
TDR	Yes	Yes
PHY External Loop Detection	Yes	Yes
CISCO-CABLE-DIAG MIB (TDR MIB)	Yes	Yes
CISCO-DATA-COLLECTION MIB	Yes	Yes
CISCO-PROCESS MIB	Yes	Yes
CPU Utilization Threshold SNMP Traps (CISCO-PROCESS-MIB)	Yes	Yes
CISCO-ERR-DISABLE MIB (port error disable)	Yes	Yes
CISCO-MAC-NOTIFICATION MIB attributes	Yes	Yes
DHCP Server	Yes	Yes
VLAN 1 Minimization	Yes	Yes
Show Interface Capabilities	Yes	Yes
RMON 1 events and alarms	Yes	Yes
Smartports I custom macros	Yes	Yes
Smartports II default macros	Yes	Yes
Smartports III global macros	Yes	Yes

SmartPort IV Enhancement	Yes	Yes
HTTP Software Upgrade	Yes	Yes
Configuration Rollback	Yes	Yes
Network Timing Protocol (NTP)	Yes	Yes
Configuration Logging	Yes	Yes
UDI - Unique Device Identifier	Yes	Yes
IP SLAs Responder	No	Yes
Configuration Replace	Yes	Yes
LLDP MED Location Support	No	Yes
LLDP MIB	Yes	Yes
LLDP_MED integration for CoS/DSCP	Yes	Yes
Cisco MAC Notification MIB	Yes	Yes
DHCP Port Based Allocation	Yes	Yes
Auto SmartPorts	Yes	Yes
Secure Copy (SCP) support for CONFIG-COPY MIB	Yes	Yes
Auto SmartPorts Phase II	Yes	Yes
DHCP option 12 for hostname configuration	Yes	Yes
LLDP MED MIB	Yes	Yes
HW External Alarm Outputs (N/C and N/O)	Yes	Yes
Wired Location Service	Yes	Yes
Industrial Ethernet Enhancements	**IA Lite (Layer 2 Lite)**	**IA BASE (Layer 2)**
Removable SD Flash (SwapDrive)	Yes	Yes
DOM Software support (SFPs w/DOM Hardware Support)	Yes	Yes
Common Industrial Protocol (CIP) Integration with Rockwell management tools	Yes	Yes
Device Manager Enhancements (Express setup, Smartports, Rockwell Automation branded)	Yes	Yes
SW Alarm relay (form "C" N/C and N/O contact outputs) and alarm subsystem integration	Yes	Yes
Industrial Automation Smartports	Yes	Yes
IEEE 1588 PTP V2	No	Yes
CIP Time Sync (CIP and 1588 integration)	Yes	Yes
CIP and DHCP integration	Yes	Yes
CIP interface	Yes	Yes
Image Download Recovery	Yes	Yes
TDR (CIP/DM Enhancements) - Broken wire detection	Yes	Yes
Resilient Ethernet Protocol (REP)	Yes	Yes
CIP Password Encryption	Yes	Yes
LLDP	Yes	Yes
CIP Enhancements (DHCP port based Allocation/CIP integration)	Yes	Yes
Profinet IO	Yes for Cisco SKU	Yes for Cisco SKU
Duplicate IP address detection	No	Yes

3.2.2 SNMP (MIB)

The following MIBs will be ported from IE3K. Please note that not all objects are supported in all of the listed MIBs

- BRIDGE-MIB
- CISCO-BRIDGE-EXT-MIB
- CISCO-BULK-FILE-MIB
- CISCO-CDP-MIB
- CISCO-CLUSTER-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-DHCP-SNOOPING-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-IETF-IP-MIB
- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB
- CISCO-L2L3-INTERFACE-CONFIG-MIB
- CISCO-LAG-MIB
- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PAE-MIB
- CISCO-PING-MIB
- CISCO-PORT-QOS-MIB
- CISCO-PORT-SECURITY-MIB
- CISCO-PORT-STORM-CONTROL-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-RTTMON-MIB
- CISCO-STACK-MIB
- CISCO-STACKMAKER-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SYSLOG-MIB
- CISCO-TCP-MIB
- CISCO-UDLDP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- IEEE8023-LAG-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB

- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RMON-MIB
- RMON2-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMP-VACM-MIB
- SNMPv2-MIB
- TCP-MIB
- UDP-MIB

3.3 Performance Requirements

Performance goals include:

1. 1588 time stamp insertion at port line speed. Clock jitter between any two consecutive IEEE 1588 devices not to exceed 100 ns

2. Ability to do NAT translation at wirespeed for control and management traffic (<5 micro second delay) *

3. NAT translation jitter between first entry and last entry in the table should be <30 micro seconds.*

4. Per flow NAT translation jitter should be <20 micro seconds.*

5. System boot time from power apply to IOS operational not to exceed 60 sec (goal is 30 sec).

6. Hardware switching/forwarding rates will be line rate

*These performance requirements for NAT are expected to be met for all protocols that are processed in HW. In the future, if there are protocols that cannot be handled completely within the FPGA and require CPU processing, then they may not be able to achieve these requirements.

3.4 Usability Requirements

New CLIs will be added to support NAT feature configuration and diagnostics. Please refer to Camaro NAT Software Functional Specification for specific new CLI options.

3.5 External Interface Requirements

The external interfaces are already described in section 2.2.4, refer to HFS for more implementation detail.

3.5.1 Required SFP List

The following table is a complete list of SFPs supported on [redacted]

SFP PID	Cisco #	Description
Ruggedized - Industrial Temperature		
GLC-SX-MM-RGD	10-2274-01	MOD,XCVR,1.25Gb/s,850nm,MM,SX,3.3V,AC,-40 to 85C,LC,SFP
GLC-LX-SM-RGD	10-2293-01	MOD,XCVR,1.25Gb/s,1310nm,SM,LX,3.3V,AC,-40 to 85C,LC,SFP,DIGITAL DIAGS
GLC-ZX-SM-RGD	10-2366-01	MOD,XCVR,1.25Gb/s,1550nm,SM,ZX,3.3V,AC,-40 to 85C,LC,SFP,DIGITAL DIAGS
GLC-FE-100FX-RGD	10-2360-01	MOD,XCVR,100Mb/s,1310nm,MM,SR,3.3V,AC,-40 to 85C,LC,SFP,100BASE-FX
GLC-FE-100LX-RGD	10-2302-01	MOD,XCVR,100Mb/s,1310nm,SM,10KM,3.3V,-40 to 85C,LC,SFP,100BASE-LX10
DOM - Extended Temperature		
SFP-GE-S	10-2143-01	MOD,XCVR,1.25Gb/s,850nm,MM,SX,3.3V,AC,-5 to 85C,LC,SFP,DIGITAL DIAGS
SFP-GE-L	10-2144-01	MOD,XCVR,1.25Gb/s,1310nm,SM,LX,3.3V,AC,-5 to 85C,LC,SFP,DIGITAL DIAGS
SFP-GE-Z	10-2031-01	MOD,XCVR,1.25Gb/s,1550nm,SM,ZX,3.3V,AC,-5 to 85C,LC,SFP,DIGITAL DIAGS
GLC-FE-100FX	10-2077-01	MOD,XCVR,100Mb/s,1310nm,MM,SR,3.3V,AC,-5 to 85C,LC,SFP
GLC-FE-100LX	10-2080-01	MOD,XCVR,100Mb/s,1310nm,SM,10KM,3.3V,-5 to 85C,LC,SFP,100BASE-LX10
GLC-FE-100EX	10-2262-02	MOD,XCVR,SFP,Ethernet,FE,125Mb/s,EX,1260-1360nm,SM,3.3V,-5 to 85C,LC
GLC-FE-100ZX	10-2263-01	MOD,XCVR,100Mb/s,1550nm,SM,80KM,3.3V,-5 to 85C,LC,SFP,100BASE-ZX
GLC-FE-100BX-U	10-2081-01	MOD,XCVR,100Mb/s,1310nm TX/1550nm RX,SM,10KM,3.3V,AC,-5 to 85C,LC,SFP,100BASE-BX10-U
GLC-FE-100BX-D	10-2101-01	MOD,XCVR,100Mb/s,1550nm TX/1310nm RX,SM,10KM,3.3V,AC,-5 to 85C,LC,SFP,100BASE-BX10-D
Commercial Temperature		
GLC-SX-MM	30-1301-03	MOD,XCVR,1.25Gb/s,850nm,MM,SX,3.3V,AC,0 to 70C,LC,SFP
GLC-SX-MM	30-1301-04	MOD,XCVR,SFP,Ethernet,GbE,1.25Gb/s,SX,850nm,MM,3.3V,0 to 70C,LC
GLC-LH-SM	30-1299-03	MOD,XCVRSFP,Ethernet,GbE,1.25Gb/s,LX,1310nm,SM,3.3V,0 to 70C,LC
GLC-BX-U	10-2094-02	MOD,XCVR,1.25Gb/s,1310nm TX/1490nm RX,SM,10KM,3.3V,AC,-5 to 70C,LC,SFP,DIGITAL DIAGS,1000BASE-BX10-U

GLC-BX-D	10-2093-02	MOD,XCVR,1.25Gb/s,1490nm TX/1310nm RX,SM,10KM,3.3V,AC,-5 to 70C,LC,SFP,DIGITAL DIAGS,1000BASE-BX10-D
CWDM-SFP-1550	10-1879-02	MOD,XCVR,125MB/s-2.67GB/s,1550nm,SM,LR,3.3V,LC,MOD20 PLUG,DIGITAL DIAGS
CWDM-SFP-1470	10-1881-02	MOD,XCVR,125MB/s-2.67GB/s,1470nm,SM,LR,3.3V,LC,MOD20 PLUG,DIGITAL DIAGS
CWDM-SFP-1530	10-1882-02	MOD,XCVR,125MB/s-2.67GB/s,1530nm,SM,LR,3.3V,LC,MOD20 PLUG,DIGITAL DIAGS
CWDM-SFP-1510	10-1883-02	MOD,XCVR,125MB/s-2.67GB/s,1510nm,SM,LR,3.3V,LC,MOD20 PLUG,DIGITAL DIAGS
CWDM-SFP-1490	10-1884-02	MOD,XCVR,125MB/s-2.67GB/s,1490nm,SM,LR,3.3V,LC,MOD20 PLUG,DIGITAL DIAGS
CWDM-SFP-1570	10-1885-02	MOD,XCVR,125MB/s-2.67GB/s,1570nm,SM,LR,3.3V,LC,MOD20 PLUG,DIGITAL DIAGS
CWDM-SFP-1590	10-1886-02	MOD,XCVR,125MB/s-2.67GB/s,1590nm,SM,LR,3.3V,LC,MOD20 PLUG,DIGITAL DIAGS
CWDM-SFP-1610	10-1887-02	MOD,XCVR,125MB/s-2.67GB/s,1610nm,SM,LR,3.3V,LC,MOD20 PLUG,DIGITAL DIAGS
DWDM-SFP-6061	10-2211-02	MOD, XCVR, 2.5Gb/s, 1560.61nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5979	10-2216-02	MOD, XCVR, 2.5Gb/s, 1559.79nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5817	10-2218-02	MOD, XCVR, 2.5Gb/s, 1558.17nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5655	10-2219-02	MOD, XCVR, 2.5Gb/s, 1556.55nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5575	10-2220-02	MOD, XCVR, 2.5Gb/s, 1555.75nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5494	10-2221-02	MOD, XCVR, 2.5Gb/s, 1554.94nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5898	10-2222-02	MOD, XCVR, 2.5Gb/s, 1558.98nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5413	10-2223-02	MOD, XCVR, 2.5Gb/s, 1554.13nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5252	10-2224-02	MOD, XCVR, 2.5Gb/s, 1552.52nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5172	10-2225-02	MOD, XCVR, 2.5Gb/s, 1551.72nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5092	10-2226-02	MOD, XCVR, 2.5Gb/s, 1550.92nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4851	10-2227-02	MOD, XCVR, 2.5Gb/s, 1548.51nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4772	10-2228-02	MOD, XCVR, 2.5Gb/s, 1547.72nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4692	10-2229-02	MOD, XCVR, 2.5Gb/s, 1546.92nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4612	10-2230-02	MOD, XCVR, 2.5Gb/s, 1546.12nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4453	10-2231-02	MOD, XCVR, 2.5Gb/s, 1544.53nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4373	10-2232-02	MOD, XCVR, 2.5Gb/s, 1543.73nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4294	10-2233-02	MOD, XCVR, 2.5Gb/s, 1542.94nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4214	10-2234-02	MOD, XCVR, 2.5Gb/s, 1542.14nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4056	10-2235-02	MOD, XCVR, 2.5Gb/s, 1540.56nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3977	10-2236-02	MOD, XCVR, 2.5Gb/s, 1539.77nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3898	10-2237-02	MOD, XCVR, 2.5Gb/s, 1538.98nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3819	10-2238-02	MOD, XCVR, 2.5Gb/s, 1538.19nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3661	10-2239-02	MOD, XCVR, 2.5Gb/s, 1536.61nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3582	10-2240-02	MOD, XCVR, 2.5Gb/s, 1535.82nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3504	10-2241-02	MOD, XCVR, 2.5Gb/s, 1535.04nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3425	10-2242-02	MOD, XCVR, 2.5Gb/s, 1534.25nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3268	10-2243-02	MOD, XCVR, 2.5Gb/s, 1532.68nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS

DWDM-SFP-3190	10-2244-02	MOD, XCVR, 2.5Gb/s, 1531.90nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3112	10-2245-02	MOD, XCVR, 2.5Gb/s, 1531.12nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3033	10-2246-02	MOD, XCVR, 2.5Gb/s, 1530.33nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4851	10-2247-02	MOD, XCVR, 2.5Gb/s, 1548.51nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3739	10-2472-02	MOD, XCVR, 2.5Gb/s, 1537.39nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-3346	10-2473-02	MOD, XCVR, 2.5Gb/s, 1533.46nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4931	10-2474-02	MOD, XCVR, 2.5Gb/s, 1549.31nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4532	10-2475-02	MOD, XCVR, 2.5Gb/s, 1545.32nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-6141	10-2476-02	MOD, XCVR, 2.5Gb/s, 1561.41nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5736	10-2477-02	MOD, XCVR, 2.5Gb/s, 1557.36nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-5332	10-2478-02	MOD, XCVR, 2.5Gb/s, 1553.32nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS
DWDM-SFP-4134	10-2479-02	MOD, XCVR, 2.5Gb/s, 1541.34nm, SM, LR2, 3.3V, 0 to 70C, LC, SFP, DIGITAL DIAGS

3.5.2 Desired SFP List

The following table has SFPs not specified in the PRD. The patch cable is required by manufacturing test and will be supported. The other listed SFPs are new and in the qualification process, they may be supported if they are qualified by the Proto 2 build cycle. Once we have final SFP designs from the vendors, these will be tested in the [redacted] skus. They will be supported at FCS if we have final designs in time for our last test cycle at P2. If not, then they will be supported in the first follow on software release once the SFPs are ready to ship.

CAB-SFP-50CM	72-4254-01	CABASY, WIRE, OEM, COPPER SFP PATCH, .5M
GLC-SX-MMD	10-2626-01	MOD, XCVR, SFP, Ethernet, GbE, 1.25Gb/s, SX, 850nm, MM, 3.3V, -5 to 85C, LC, DOM, BP
GLC-EX-SMD	10-2529-01	MOD,XCVR,1.25Gb/s,1310nm,SM,EX,3.3V,-5 to 85C,LC,SFP
GLC-LH-SMD	10-2625-01	MOD, XCVR, SFP, Ethernet, GbE, 1.25Gb/s, LX, 1310nm, SM, 3.3V, -5 to 85C, LC, DOM, BP
GLC-ZX-SMD	10-2621-01	MOD, XCVR, SFP, Ethernet, GbE, 1.25Gb/s, ZX, 1550nm, SM, 3.3V, -5 to 85C, LC, DOM, BP
GLC-FE-100BX-URGD	10-2414-01	MOD, XCVR, 100Mb/s, 1310nm TX/1550nm RX, SM, 10KM, 3.3V, AC, -40C to 85C, LC, SFP, 100BASE-BX10-U

3.5.3 Not Supported SFP List

The following table has SFPs which will not be supported on the Camaro project. They include the Huck Finn and Tom Sawyer SFPs.

GLC-GE-100FX	10-2019-01	MOD, XCVR, 100Mb/s, 1310nm, MM, SR, 3.3V, AC, 0 to 70C, LC, SFP
GLC-T	30-1410-01	MOD, XCVR, ELECTRICAL, 10/100/1000BASE-T, SR, 3.3V, RJ45, MOD20 PLUG
GLC-TE	?	MOD, XCVR, ELECTRICAL, 10/100/1000BASE-T, SR, 3.3V, AC, 0 to 85C, RJ45, SFP, BP
SFP-GE-T	30-1421-01	MOD, XCVR, ELECTRICAL, 10/100/1000BASE-T, SR, 3.3V, AC, 0 to 85C, RJ45, SFP,

3.6 Architecture Baseline Requirements

The [redacted] family of Industrial Ethernet switches shares its SW architecture and basic HW architecture with the existing IE3000 platform. The processor complex and a switch ASICs are based on the Sasquatch ASIC family used in the IE3000, and the SW will release from the same IOS branch or a child of that branch. From an architecture baseline perspective the [redacted] family will be consistent with the IE3000 platform and other ESTG L2 switches built from the Sasquatch switch ASIC or its derivatives.

Since [redacted] SW will be leveraged from existing IE3000 platform, no gap analysis will be performed for this project.

3.7 Carrier Class Requirements

[redacted] (IE2K/S7K) is not directly targeted for the Service Provider market and as such no Carrier Class requirements are specified per section 6.10 of the PRD.

3.8 Mechanical Description

There are 4 mechanical sizes of Camaro SKUs. The following sections describe each of the 4 mechanical sizes.

SIZE TABLE

SKU	Current Design Size (Front of DIN Rail)	Current Design Size (Back of DIN Rail)
Z4, Z4G, Z4S, Z4SG	5.100 high x 2.945 wide x 4.300 deep	5.100 high x 2.945 wide x 4.595 deep
Z8, Z8G	5.100 high x 3.600 wide x 4.300 deep	5.100 high x 3.600 wide x 4.595 deep
Z8E	5.100 high x 3.600 wide x 5.050 deep	5.100 high x 3.600 wide x 5.345 deep
Z16, Z16GE, Z16GEX	5.100 high x 5.000 wide x 5.050 deep	5.100 high x 5.000 wide x 5.345 deep

3.9.1 Compliance

Here is an extensive list of compliance standards that are eclipsed by the standards below.

Type	Standards
Electromagnetic Emissions and Immunity Compliance (EMC)	FCC 47 CFR Part 15 Class A EN 55022A Class A VCCI Class A AS/NZS CISPR 22 Class A and AS/NZS CISPR 24 CISPR11 Class A, CISPR22 Class A ICES 003 Class A KCC -Korea CE Marking C-Tick (Australia) Russia certification Brazil Compliance RoHS compliance China (CCC) Tiawan CNS 13438 class A (BMSI) EN-61000-4-2 (Electro Static Discharge), 15Kv air/8Kv contact EN 61000-4-3 (Electro Magnetic field, 10 and 20V/m) EN 61000-4-4 (Fast Transients – 4 KV power line, 4 KV, data line EN 61000-4-5 (Cisco IE2K / S7K – 2 KV/1 KV for DC EN-61000-4-6 (Conducted Immunity, 10V/emf) EN-61000-4-8 (Power Frequency Magnetic Field Immunity) EN-61000-4-9 (Pulse Magnetic Field Immunity) EN-61000-4-10 (Oscillatory Magnetic Field Immunity) EN-61000-4-11 (AC power Voltage Immunity) EN-61000-4-29 (Voltage Dips Immunity) EN61000-6-2 (Immunity for Industrial Environments) EN 61000-6-4Class A EN 61000-6-1 (Immunity for Light Industrial Environments) EN61326
Humidity	Cisco IE2K / S7K should meet or exceed relative humidity of 5% to 95% non-condensing.

	IEC 60068-52-2(Salt Fog Mist, Test Kb) Marine environments IEC 60068-2-3 IEC 60068-2-30
Shock and Vibration	Shock: 30g, 11ms Operational Vibration: 2g@10 – 500hz Trapezoidal Pulse Shock 65G per ASTM D3332, non-operational IEC 60068-2-27 (Shock) IEC 60068-2-31 (Shock) IEC 60068-2-32 (Shock) IEC 60068-2-64 (Vibration) IEC 255 21.1 Class 1
Safety standards and certifications	
Information Technology Equipment	UL/CSA60950-1 EN 60950-1; TUV/GS CB to IEC 60950-1 with all country deviations NOM to NOM-019-SCFI (through partners and distributor) CE Marking
Industrial (Control Equipment) Floor	UL 508 CSA C22.2, No 142
Hazardous Locations	IEC 60079-0, -15 (IECEx test report from Demko, Class I,Zone 2 A-D) EN 60079-0, -15 ATEX certification (II, 3G,Zone 2) InMetro (pending final decision) ANSI/ISA-12.12.01-2007 (Class I, Div 2 A-D) CSA C22.2, No 213 (Class I, Div 2 A-D)
Noise Specifications	Office Product Spec: 50Dba
Industry Standards	EN61131-2 (Programmable Controllers) Protective Coating Lloyd's Register Type Approval – ENV2 or ENV3 British, German Lloyds RA 156 -165 MHz 24 dBuV/M – Class A is 50dBuV/M – Marine band) ODVA Industrial EtherNet/IP Marine (LR, BV, GL, DnV, Rina ABS, KR) or IACS wheel mark Substation (IEEE 1613, IEC 61850-3), KEMA Railway (EN50155), EN50121-4 NEMA TS-2 IP20 (per EN60529) IP 30 and higher levels should be evaluated.
Operating Environment	It is required that all Cisco IE2K / S7K base SKUs meet or exceed an operating temperature of -40^{0}C to + 75^{0}C (A temperature rating of -40C to 70C is required for conformally coated versions).

	Operating Temperature: -40C to +60C (Hazardous Location) Operating Temperature: -40C to +70C (General Applications and Power Substations, IEC 870-2-2 Class C3) Operating Temperature: -40C to +75C (NEMA TS-2 with a fan or blower equipped enclosure, 100 CFM minimum airflow) EN 60068-2-1 EN 60068-2-2 EN 61163 Altitude: up to 15,000 feet **See Section 3.9.1.5 for more details**
Storage Environment	Temperature: -40 to +85 degrees C IEC 600068-2-14 Altitude: 15,000 feet
Corrosion	ISO 9223: Corrosion class C3-Medium ISO 9223: Corrosion class C4-High
Oil Resistance	Resistant to lubricants specified in DMS:901784, EN 60811-2-1
Lightning Protection	IEC 61400-24, Wind Turbines – Part 24
Others	TAA (Government)

Required Markings on product label – c-UL-us, CE, C-Tick, Ex, Ethernet/IP, INMETRO, CCC, KCC, IACS Wheel mark(Marine), CE mark

3.9.1.1 Country Approvals/Certifications

Many countries have their own requirements and approval process that must be met before Cisco can export to them:

Country	*Timeline*	*Comments*
Canada	FCS	
U.S.A.		
Japan		
Australia		
New Zealand		
CE Countries		
Korea	After FCS, by 3 months	For certification
China	After FCS, by 6 months	For certification
Brazil	After FCS, by 6 months	For certification
Taiwan	After FCS, by 3 months	For certification
KEMA	After FCS, by 6 months	
TS/2	After FCS, by 6 months	

Railway	After FCS by 6 months	
Vestas	After FCS, by 3 months	To meet by FCS if possible

3.9.1.2 Regulatory Requirements IEC 61850

REQ Tag	*Requirement*	*Reference*
NA	*EMC*	Cisco IE2K / S7K with all its platforms, accessories and components must comply with applicable EMC Standards and obtain all approvals required by each country where the product is marketed, sold and used prior to FCS. If there is a delay in obtaining few country approvals, FCS should not be delayed. Please refer to the above compliance table for details.
NA	*Safety*	Cisco IE2K / S7K with all its platforms, accessories and components must comply with applicable Safety Standards and obtain all approvals required by each country where the product is marketed, sold and used prior to FCS, except for Brazil and China. For field trials, Cisco IE2K / S7K must meet the Safety Standards for the country in which the product will be used. Please refer to the above compliance table for details.
NA	*Wireless*	*NA*
NA	*PTT*	Cisco IE2K / S7K with all its platforms, accessories and components must comply with applicable PTT Standards and obtain all approvals required by each country where the product is marketed, sold and used.

3.9.1.3 Customer Requirements

In general there are no customer specific requirements as part of the program. The general requirements were based on target markets/customers. The table below lists the requirements (that are called out elsewhere) that were mostly driven by specific customers.

Example: Customer Requirements Table

REQ Tag	Requirement	Reference
NA	Conformal Coating	*Vestas requires conformal coating on 16 port sku*

3.9.1.4 Corrosive Testing

The IE-2000-16TC-G-X is the only sku that will be required to pass the corrosive tests.

3.9.1.4.1 Corrosive tests:

The IE-2000-16TC-G-X Mechanical components/housing protective coatings must pass: **ISO 12944-6.**

C3-High Classification (more than 15yrs)

Mechanical components/housing protective coatings and the PCA assembly must pass: Salt Spray test **IEC 60068-2-52**, salt mist test.

Severity 2

PRODUCT EXPOSED TO THE MARINE ENVIRONMENT FROM TIME TO TIME BUT WILL NORMALLY BE PROTECTED BY AN ENCLOSURE, E.G. NAVIGATIONAL EQUIPMENT WHICH WILL NORMALLY BE USED ON THE BRIDGE OR IN A CONTROL ROOM

Test Duration 3 Days per Sev 2 test in spec

Mechanical components/housing protective coatings and the PCA assembly must pass: Airborne contaminants **IEC 60068-2-60**

Test Method 3 (Cl2, NO2,and H2S)

Test Duration 21 Days

Preferred durations in the specification are 4, 7, 10, 14 and 21 days. We need to understand where the 31 days per Marketing request came from.

The PRD calls out testing to G3. G3 is not a class in the specification. As stated. we will test to Method 4

Copper reactivity monitoring should reflect approximately a 3300 Angstrom thickness during one day of testing.

Mechanical components/housing protective coatings and the PCA assembly must pass:

Salt Spray test: ISO 7253 for 480 hours. This has been preceded by ISO 9227:2006. Only NSS (Neutral Salt Spray) applies to our metals, as AASS (acetic acid salt spray) and CASS (copper-accelerated acetic acid salt spray) applies to materials with Chromium which we do not have since we are RoHS 6/6. We need to agree with the customer BEFORE testing on the shape

and orientation of the metallic parts in the test chamber, and also agree with the customer about pass/fail criteria.

Mechanical components/housing protective coatings and the PCA assembly must pass:

Water Condensation test: ISO 6270 for 240 hours.

3.9.1.4.2 Pass/Fail Criteria:

- Functional or test failuresof assembly after corrosive tests will constitute a fail.
- Re-test EMI and transient tests before visual inspection. These tests must pass per their respective test plans.
- Perform visual inspection per IPC-A-610 Section 10.8 to verify there are no visual failures of the assembly after completion of corrosive tests. A visual failure also includes, but is not limited to, significant change in finish and or color from original finish and color.
- For IEC60068-2-60 Method 3: Copper reactivity monitoring should reflect approximately a 3300 Angstrom thickness during one day of testing.

3.9.1.4.3 Conformal Coating:

If conformal coating is required to pass these tests, the conformal coating material must be UL746E recognized with a UL94 V0 rating.

Examples of some acceptable CC materials are:

- Humiseal Silicone 1C51
- Humiseal AR/UR UV40
- Humiseal Silicone 1B73

3.9.1.5 Thermal Requirements

Continuous Operating Temperature Range, All Non-Conformally Coated SKU's

Application	General Applications and Power Substations [1]		Industrial Automation[3]	Traffic Signal NEMA TS-2
Temperature Range	-40C to +70C continuous; 85C limited duration [2]		-40C to +60C	-40 to +75C
Installation Environment	Vented Enclosure	Equipment closet, free air, relay rack, and panel mount	Sealed Enclosure	Fan Equipped Enclosure [4]
Environment Dimensional Requirements (Depth x Width x Height)	The minimum enclosure internal dimensions are: 12 x 24 x 24 in (30 x 61 x 61 cm). Enclosure examples are NEMA1, IP20, and IP21	The minimum internal dimensions of installation closet, enclosure, or room is 16 x 24 x 60 in (41 x 61 x 152 cm)	Minimum enclosure internal dimensions are 9 x 18 x 18 in (23 x 46 x 46 cm). Enclosure examples are NEMA4 and IP54	Maximum cabinet dimension is 24 x 44 x 72 in (61 x 112 x 183 cm) [5]

1. Power substations requirements are tested according to the operating temperature range of -40C to +70C described in IEEE 1613 section 4.1.1 when tested according to the configuration described in IEC 60068-2-2, section 3.1 "low air velocity in the working space." This also meets the requirements as described in IEC 870-2-2 Class C3.
2. 85C Type Test: The unit shall function as specified after operational environmental exposure of 85C for 16 hours duration in the installation environments shown for vented enclosure, equipment closet, free air, relay rack, and panel mount.
3. In accordance with UL 60950-1, section 1.7.17, the product must be installed in a "RESTRICTED ACCESS LOCATION." During operation, the surface temperature will exceed the maximum permissible temperature for equipment installed in "OPERATOR ACCESS AREAS."
4. In accordance with NEMA TS-2 section 7.9.1, the ventilation fan must deliver a minimum of 100 CFM airflow.
5. In accordance with NEMA TS-2 section 7.3, all standard enclosure sizes are supported.

Continuous Operating Tempaere Range, All Conformally Coated SKU's

To meet thermal requirements, all conformally coated SKU's maximum temperature ratings are derated by 5 degrees C from the non-conformally coated SKU's for each respective installation environment.

Installation Method

To meet thermal requirements, the unit must be installed using DIN Rail (EN 50022) or supported bracket kit for rack mounted and panel mounted installations.

Clearance Requirement

To meet thermal requirements, the units must have a minimum of 1 inch (25mm) clearance to the nearest unit on the left and right side and a minimum of 3 inches (76mm) clearance to the nearest unit on the top and bottom.

** The Camaro skus are designed to, and will be thoroughly tested to, the above specs. If testing shows that there is enough margin that these specs can be extended, then the ranges will be extended as applicable.*

3.9.1.6 Accessibility Design Requirements

[redacted] is classified as "back office" product, not touched by end users, so the hardware (chassis & cards) are exempt from accessibility requirements as per 1194.3(f) of the US Section 508 of the Rehabilitation Act.

The physical hardware is exempt, and the remote administration is covered by IOS "The IOS Command Line Interface (CLI) is fully compatible with all text-to-speech PC screen readers and therefore meets the U.S. GSA interpretation of Section 508 that a back office product be fully accessible to a low-vision or blind remote network administrator." so there's no administrative accessibility change to consider." IOS has a separate VPAT with EDCS-486209 for the "remote administrator" requirements.

Relevant Accessibility Regulations & Laws are specified in Cisco Accessibility Design Requirements at

http://wwwin.cisco.com/accessibility/requirements/

From a software perspective, exact implementation of the web management tool is TBD, but the high level requirements are listed in Section 6.5.

The Web Management will need assessed using the Cisco Web ADR (see http://wwwin.cisco.com/accessibility/requirements/web_adrs/main.html). Cisco Web ADR requirements for CMA and LMS/Lumous ADR requirements will be documented in their respective PRDs.

Section 508 provides an exemption clause. It states that under certain conditions, a product is exempt and does not have to meet accessibility laws and regulations.

A product is exempt from meeting accessibility laws and regulations if:

1. It is **back office equipment**. A back office is sometimes called a wiring, equipment, or restricted access closet. These are spaces frequented only by service personnel for maintenance, repair, or occasional monitoring. The reason for this exemption is that the back offices can present safety hazards for a person with a disability, for instance, the presence of DC electrical power cords. Data centers are considered "back offices".

   However, if the back-office product can be monitored and serviced remotely, the remote features must be made accessible to people with disabilities. Therefore, most Cisco products are not exempt.

   Also, although a product may qualify for this exempt status, the product documentation must be accessible. This is because people with disabilities can and do hold jobs such as TAC Support or a Call Center Administrator where having information about the equipment is critical to their job even though the equipment resides in a back office.

2. It is **under contract to the US Federal Government** for systems in direct support of national security, military forces, or weapons systems, and NOT used by civilians. Military personnel typically must meet a rigorous standard of physical ability. In this case, the documentation is exempt as well. However, this standard does not exclude people who are color blind, so even these products should be accessible and usable by people with color blindness.

Hardware Checklist - Revision 8, 2005-JAN-31					
ID	**Description**	**Requirements Level**	**Applies to (T, G, V, or All)**	**Status**	**Comments**
ACC-HW-10	**Controls: buttons, keys, latches, etc.**				
ACC-HW-10.11	Provide controls with low force requirements.	Must	**All**	**PASS**	
ACC-HW-10.31	Provide keys which are tactilely discernible without activating them, or equivalent controls for touchscreens.	Must	**All**	**N/A**	**No keys**
ACC-HW-10.41	Provide large, well-spaced controls.	Should	**All**	**N/A**	**No active controls**
ACC-HW-10.51	Reduce the possibility of accidental activation.	Should	**All**	**PASS**	
ACC-HW-10.61	Provide the status of all locking or toggle keys visually and either through touch or sound.	Must	**All**	**N/A**	**No locking/toggle keys**
ACC-HW-10.71	Do not require an end-user to attach assistive technology to the product.	Must	**Applies only to public products like ATMs and kiosks.**	**N/A**	**Not a public product**
ACC-HW-10.81	Provide alternative forms of user identification for biometric identification.	Must	**All**	**N/A**	**No biometric identification**
ACC-HW-20	**Handsets and other grasped and held objects**				
ACC-HW-20.11	Provide users with reduced mobility a way to approach the product and reach all controls.	Must	**For permanently installed**	**N/A**	**No handsets or held objects**

			products (ATMs, etc.)		
ACC-HW-20.21	Provide for easy grasping, holding, and manipulating where necessary.	Should	All	N/A	No holding required
ACC-HW-30	Alternate external connections				
ACC-HW-30.11	Provide industry standard ports for alternative input and output devices.	Must	T, V	N/A	Product is in the G category
ACC-HW-30.21	Make sure that all connectors are easy to connect and disconnect.	Should	T, V	N/A	Product is in the G category
ACC-HW-40	Visual				
ACC-HW-40.11	Use color as an enhancement, but not as the only way to distinguish controls and labels.	Must	All	PASS	Meets Cisco port labeling standards
ACC-HW-40.21	Avoid hardware that would cause a visible flicker with a frequency greater than 2 Hz and lower than 55 Hz.	Must	All products with displays	N/A	No displays
ACC-HW-40.31	Provide for sufficient contrast control of displays.	Should	All products with displays	N/A	No displays
ACC-HW-40.51	Provide audio description hardware for video playback where necessary.	Must	V	N/A	No video playback
ACC-HW-40.61	Design displays and labels to minimize the effect of glare.	Should	All	PASS	Front label is low-glare finish
ACC-HW-40.71	Select LCDs and similar displays to allow large, easy to read characters.	Should	All products with displays	N/A	No displays
ACC-HW-50	Sounds				
ACC-HW-50.11	Provide a volume control.	Must	All products with audio output	N/A	No audio outputs
ACC-HW-50.21	Provide a function to reset the volume to the default level after every use.	Must	T	N/A	No audio outputs
ACC-HW-50.31	Provide an industry standard audio connector to allow for private listening and amplification.	Must	All products with audio output	N/A	No audio outputs
ACC-HW-50.41	Provide captioning hardware where necessary.	Must	V	N/A	No audio outputs
ACC-HW-60	Testing				
ACC-HW-60.11	Test for accessibility using available tools.	Must	All		

Software Non browser-based GUI Checklist - Revision 6, 2005-JAN-31				
ID	Description	Requirement Level	Status	Comments
ACC-SW	Keyboard, Mouse, and Other Input			
ACC-SW-10.11	Provide keyboard equivalents and other user input options for all actions.	Must		
ACC-SW-10.21	Do not interfere with input accessibility features built into the operating system.	Must		
ACC-SW-10.31	Provide the ability to remap keyboard equivalents.	Should		

ACC-SW-10.41	Provide compatibility with alternate input devices and systems.	Must		
ACC-SW-10.51	Provide a keyboard method to navigate to all objects.	Must		
ACC-SW-10.61	Avoid requiring multiple simultaneous keystrokes (chorded key presses) and pressing a key for an extended period of time.	Must		
ACC-SW-10.71	Provide users with the ability to correct input errors.	Should		
ACC-SW-10.81	Do not provide automatic key repeat.	Must		
ACC-SW-10.91	Provide audio and visual feedback that input has been received and is being processed.	Should		
ACC-SW-20	**Object Information**			
ACC-SW-20.11	Apply a visible focus to a default object in each window of the application.	Must		
ACC-SW-20.21	For all non-text objects that convey information (such as a graph), provide a text description that can be read by a screen reader.	Must		
ACC-SW-20.41	Use meaningful and consistent labels for all objects.	Must		
ACC-SW-30	**Sounds and Multimedia**			
ACC-SW-30.11	Display a visual cue for all audio alerts.	Must		
ACC-SW-30.21	Provide accessible alternatives to all audio and video that contains information.	Must		
ACC-SW-30.31	Support volume settings in the operating system or provide volume control.	Must		
ACC-SW-30.41	Select or design audible elements that are easy to hear, recognize, and understand.	Should		
ACC-SW-50	**Visual Content**			
ACC-SW-50.11	Provide text in a manner compatible with assistive technology, or make the product able to provide the assistive technology functionality itself.	Must		
ACC-SW-50.21	Use color as an enhancement, but not as the only way to convey information or indicate an action.	Must		
ACC-SW-50.31	Allow the user to control the font, size, color, and contrast of the entire user interface.	Must		
ACC-SW-50.41	If the application lets users select colors, provide a variety of color selections capable of producing a range of contrast levels.	Must		
ACC-SW-50.51	Select or design formatting and graphical elements that are easy to recognize and understand.	Should		
ACC-SW-50.61	Provide an option to display animated information, including moving text, in a non-animated presentation mode.	Must		
ACC-SW-60	**Timing**			
ACC-SW-60.11	Do not use timeouts, or provide a timeout warning to the user and a way for the user to extend the response time.	Must		
ACC-SW-60.21	Avoid the use of blinking or flashing objects.	Must		
ACC-SW-60.41	Do not use timeouts for user instructions or prompts.	Should		
ACC-SW-70	**Verify Accessibility**			
ACC-SW-70.11	Test for accessibility using available tools.	Must		

3.9.2 Design Specifications for Product Identification

[redacted] project will comply with all UDI requirements, PID assignments have been made and labels/IOS inventory/MIB compliance will be verified at pre-pilot build. A separate UDI compliance document will be added to EDCS detailing this.

3.10 Public Sector Design Requirements

There are no Public Sector requirements required in the PRD for Camaro.

3.11 Quality Requirements

Unique Requirement ID	Requirement Detailed Description	Required/ Optional	Requirement Type	Comment
QUALITY10	Product must adhere to Reliability Demo. Test (RDT) EDCS-7005770	Required	Global	
QUALITY11	MTBF calculation must meet or exceed MTBF target at Gate Review (CC & Final TRR)	Required	Global	

3.11.1 Security Requirements

There are no specific Security requirements for Camaro.

3.11.2 Reliability/Availability Requirements

The MTBF target is to exceed 42.7 Years or 374,052 hours for each sku.

Current MTBF estimates are shown in the table below:

ASSEMBLY NUMBER	-REV	DESCRIPTION	COMP. QTY	MEAN FIT	SD FIT	Issue 2 FIT	Issue 2 MTBF	BOM STATUS	FIT CALC. STATUS
800-35619-01	-17	ASY,ELMECH,CAMARO,IE2000-8TC-G-E,1588	1,526	5,077.02	776.75	6,094.43	458,176	OK	Complete
800-35623-01	-16	ASY,ELMECH,CAMARO,IE2000-16TC, 4x100Mb	1,896	7,725.06	1,071.53	9,126.16	414,044	OK	Complete
800-35617-01	-16	ASY,ELMECH,CAMARO,IE2000-8TC	1,398	4,798.65	774.07	5,813.54	535,935	OK	Complete
800-35621-01	-15	ASY,ELMECH,CAMARO,IE-2000-4TS	1,346	3,580.50	571.10	4,329.12	540,054	OK	Complete
800-35615-01	-14	ASY,ELMECH,CAMARO,IE2000-4T	1,295	3,554.22	571.07	4,302.91	547,859	OK	Complete

3.11.2.1 Reliability/Availability Budget

This product is not a modular chassis and thus does not need availability budgeting.

3.11.2.2 Online Insertion and Removal

No specific requirements per PRD section 10.6

3.12 Serviceability Requirements

PSD Serviceability Requirements for IE2K-[redacted] (IE2K/S7K)

P1 = Must Have
P2 = Desirable
Accepted/Rejected:

Number	Requirement ID	Requirement Description	Priority	**Owner/Comments**	Accepted/Rejected	NSSTG Comments
1.	IE2K-PSD-WS-2	IE2K switch shall support IOS conditional debugging. This includes access control lists and timers.	P1	To the extent supported by IOS infrastructure. Support for ACL and timers will be the same as on IE3K platform.	Accepted	
2.	IE2K-PSD-WS-3	For debugs related to Clients, provide the ability to bind an Access Control List (ACL) comprised of MAC addresses, to debugs. For example, debug dhcp client <access-list>	P1	To the extent supported as on IE3K platforms	Accepted	
3.	IE2K-PSD-WS-4	Provide detailed yet human	P1	N/A. This feature is currently not supported on	Rejected	

		readable CAPWAP debugs, e.g. debug capwap {event | error | packet}		IE3000.		
4.	IE2K-PSD-WS-11	There should be High Availablility (HA) within an IE2K stack.	P1	N/A. IE2K is standalone box.	Rejected	
5.	IE2K-PSD-WS-7	There should be full support for IOS's show interface including packets in and out, multicast and broadcast, queue depths, drops, errors, and so forth.	P1	To the extent supported as on IE3K platforms	Accepted	
6.	IE2K-PSD-WS-13	There should be sufficient local storage capacity to hold an entire "crashinfo" file and Coredump. Additional Details: Whether disk, flash, NVRAM, etc. – a local	P1	Camaro SW will support the ability to locally store the crashinfo, coredump as in IE3K platform. The crashinfo file will be stored in the on-board flash.	Accepted	

		IFS device that can hold the entire crashinfo (with room to spare), is necessary, so that "crashinfo" does not have to be transmitted over the network at the time of an actual crash event.				
7.	IE2K-PSD-WS-16	There should be support for debug {ip | tcp | udp | icmp} packet [access-list] [detail | error] [dump] Additional Details: There should be an ability to monitor traffic through the system. For example the user should be able to see how many packets went to a specific subnet, where he is dropping packets and where he is	P1	Supported to the extent that it is supported in the IE3K lanbase image, which does provide some level of debug (i.e. for QoS) but not to the granularity mentioned here.	Rejected	

		running into QoS issues.				
8.	IE2K-PSD-WS-17	There should be SPAN (Switch Port Analyzer) functionality for interfaces.	P1	Camaro SW will support this functionality as in IE3K platform	Accepted	
9.	IE2K-PSD-WS-18	There should be R-SPAN (Remote SPAN) functionality for interfaces.	P2	To the extent supported as on IE3K platforms	Accepted	
10.	IE2K-PSD-WS-19	There should be ELAM capture capability for packets to and from the ASIC.	P2	HW limitation	Rejected	
11.	IE2K-PSD-WS-20	There should be Embedded Packet Capture (EPC) functionality. Additional Details: Refer to EDCS-481241 and EDCS-578236. There should be Router IP Export (RITE). Additional Details: Refer	P1	Currently not supported in IE3000 LanBase	Rejected	

		to EDCS-247807.				
12.	IE2K-PSD-WS-22	Nvgen all non-default configuration.	P1	To the extent supported as on IE3K platforms	Accepted	
13.	IE2K-PSD-WS-23	Commands to configure the system should for the most part not require a reload in order to take effect in production or to work properly and document the ones that require a reload.	P1	To the extent supported as on IE3K platforms	Accepted	
14.	IE2K-PSD-WS-24	There should be support for Control Plane Policing. (Refer to EDCS-216047 and EDCS-338734)	P2	Not supported in the IE3K baseline.	Rejected	
15.	IE2K-PSD-WS-25	All logs, messages, and debugs, should conform to IOS standards, including, but	P1	Will conform to IOS standards. Will have same support as in IE3K platform	Accepted	

		not limited to: logging to local buffer, Severities 1 to 8, and support for timestamps to the millisecond.				
16.	IE2K-PSD-WS-30	There should be a password recovery procedure that does not require erasure of the entire configuration.	P1	As on the IE3K, pwd recovery requires clearing the config.	Rejected	
17.	IE2K-PSD-WS-31	Ensure that all proposed CLI conforms to Cisco's Parser Police Manifesto, and has been approved by the parser-police alias.	P1	SW	Accepted	
18.	IE2K-PSD-WS-32	Ensure that all SNMP MIBs have been reviewed by the mib-police alias.	P1	SW	Accepted	

19.	IE2K-PSD-WS-40	Provide a method to easily to isolate a faulty stack port (or flapping stack link).	P1	N/A. IE2K is standalone	Rejected	
20.	IE2K-PSD-WS-41	In case of stacking there should be an ability to read statistics of all the stack ports.	P1	N/A. IE2K is standalone	Rejected	
21.	IE2K-PSD-WS-42	"***Sh version***" should display actual physical DRAM on Sup card. Currently it does not list the Memory used by Linux.	P1	Camaro will show the processor memory as current support on IE3K	Accepted	

Applicable CA input requirements defined in the CA Input Workbook (EDCS-338888) must be met:

Requirements

Since there will be no new development in the following functionalities, [redacted] SW will meet the following requirements, if applicable, to the extent of the IE3000 support.

ReqProID	Requirement Name	Requirement

PRODSEC41	**SEC-STA-AUDIT**	**Startup and shutdown audit records**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that have logging or audit processes. **Requirement:**There **MUST** be audit records for startup and shutdown of the auditing process itself. If the auditing process is always active whenever the PRODUCT itself is running and cannot be disabled by configuration, then logging of PRODUCT startup and shutdown is sufficient to fulfill this requirement. **Status:** Current **Justification:** Requirement for Common Criteria security targets **Document References:** DOD Protection Profile for medium robustness for firewalls - FAU_GEN.1 Audit data generation Implementation Guidelines**: None**	
PRODSEC42	**SEC-AUD-FIELD**	**Audit record fields**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that support logging or auditing. **Requirement:** Each audit record **MUST** include: Date and time of the event, time zone, type of event, subject identity (user identity and/or source address), and the outcome (success or failure) of the event, except as described in SEC-USR-MESS. **Status:** Current **Justification:** Requirement for Common Criteria security targets **Document References:** DOD Protection Profile for medium robustness for firewalls - FAU_GEN.1 Audit data generation; Network Security Requirements for Devices Implementing Internet Protocol **Implementation Guidelines:** None	
PRODSEC43	**SEC-LIM-MESS**	**Rate limit or aggregate audit messages**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that support logging or auditing. **Requirement:** PRODUCTS **MUST** have the capability to rate limit or aggregate audit messages. **Status**: Current **Justification:** There is the potential to overwhelm the audit server, or cause the device to be so busy sending repetitive audit messages that functions are impaired. **Document References:** **Implementation Guidelines:** None	
PRODSEC44	**SEC-USR-MESS**	**Username in audit message**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that support logging or auditing. **Requirement:** In a password system for an authentication failure, the username **MUST** be checked and, if valid, **MUST** be included in the audit message. If the username is not valid, then the string **MUST** be excluded in the audit message. When a PRODUCT is doing logging while using an external AAA server to provide the credential check and gets back a failure with no indication of the correctness of the username, then the string **MUST** be excluded in the audit message. **Status:** Current **Justification:** Users will sometimes accidentally type their valid password in the space	

	designated for username. Since we do not want to record any passwords in a log file, we should not record an invalid username. **Document References:** **Implementation Guidelines:** None	
PRODSEC45	**SEC-PWD-AUDIT**	**Exclude password in audit record**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that support logging or auditing. **Requirement:** Passwords **MUST** be excluded from all audit records including records of successful or failed authentication attempts. **Status**: Current **Justification:** Passwords should not be stored in log files because it may allow unauthorized users to access these passwords during audits of log records, and also makes the Syslog server a more desirable target for attackers. **Document References:** **Implementation Guidelines:** None	
PRODSEC46	**SEC-CHG-LOGD**	**Changes to logging configuration always logged**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that support logging or auditing. **Requirement:**Whenever any form of logging is in operation, all changes to the configuration of the logging service itself **MUST** be logged in a reliable manner. For the purposes of this requirement, "changes to the configuration of the logging service" includes: • enabling or disabling logging, • changes in logging servers or other log data destinations, • changes to the logging protocols or to the configurations of those protocols, • changes in system wide logging filters, • changes to the logging severity or priority assigned to logging-related events such as loss of log data, • changes to the system's response to the exhaustion of logging resources, changes in the sizes of logging buffers, • other changes which might cause log entries to be lost, hidden, or misdirected. **Status:** Current **Justification:** If the logging configuration can be changed without the change itself being recorded, the integrity of logs can easily be compromised. **Document References:** **Implementation Guidelines:** This is not meant to require the detection of changes to the stored logging configuration while the logging service itself is shut down.	
PRODSEC47	**SEC-ALL-LOGD-2**	**Events loggable to SYSLOG**
	Condition: This behavior is **MANDATORY** for all PRODUCTS that support logging or auditing. **Requirement:** Each PRODUCT **MUST** be capable of logging auditable events using Syslog and/or acknowledged Syslog, in addition to any other method. The determination for using Syslog or acknowledged Syslog is by user configuration. **Status:** Current **Justification:** Administrators generally prefer to have all logging information available in one place.	

	Document References: **Implementation Guidelines:** This requirement states events that already have log messages need to be able to be sent via Syslog. It does not require making every event auditable. For example, AAA events and events generating SNMP traps should be loggable via Syslog.	
PRODSEC72	**SEC-ACC-CRED**	**Remote access not allowed without credential**
	Condition: This requirement is **MANDATORY** for all STANDALONE DEVICES. **Requirement:** Without a password, SNMP community string, or other authentication credential being set by the customer, remote access **MUST** be disallowed. SNMP MUST be disabled and remain disabled until a community string is set and the service is turned on. Any remote interactive connection, such as a TELNET connection, **MUST** be refused or the service disabled until a password is set. **Status:** Current **Justification:** With the default of no community strings being set, it is important to make sure that the device is in a secure state, and unauthorized access is not allowed. This supports the goals of least privilege and confidentiality. **Document References:** ENG-83132 Product Security Design Requirements; http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shmtl http://www.cisco.com/warp/public/707/ios-snmp-community-vulns-pub.shtml **Implementation Guidelines:** For devices which have a separate command to turn on the SNMP service, it must be configured on as well as the community strings set for SNMP to be enabled and respond to queries.	
PRODSEC48	**SEC-BAN-INFO**	**Limiting information in banners**
	Condition: This requirement is **MANDATORY** for all PRODUCTS supporting logins through any interactive user interface such as text-mode (terminal-mode) connections or HTTP. **Requirement:** When an interactive connection is made to the Product, regardless of the protocol used, the banner information displayed to the user before login **MUST**, by default, be free of any information identifying the Product, the software or version of software running on the Product, or any information identifying the particular instance of the PRODUCT to which the connection is being made, such as a serial number or a customer-assigned host name. **Status:** Current **Justification:** Any information that is given may help an intruder determine the applications or services running, operating system and other information that could be useful in attacking the device or system. **Document References:** Report Number: C4-040R-02, Router Security Configuration Guide, National Security Agency, September 27, 2002 **Implementation Guidelines**: It is not possible to remove all potentially detectable differences between products, but, it should be possible at least to make software versions difficult to infer. For new products supporting terminal-style connections, the best choice is generally to use the "User Access Verification" banner used by IOS. Future versions of this specification may standardize the terminal-mode and HTTP banners.	
PRODSEC7	**SEC-BE-STABLE**	**Remain stable during flooding attack**
	Condition: This requirement is **MANDATORY** for all STANDALONE DEVICES. **Requirement:** During a REFERENCE FLOOD directed to or through the device, the STANDALONE DEVICE **MUST** remain stable which means continuing to operate without reloading its software, and maintaining the integrity and consistency of its internal data structures, and the device **MUST** recover gracefully after the attack has ended. No	

	human intervention **MUST** be required. **Status:Mandatory** **Justification:** Devices, which can be crashed or disabled for the long term, are major targets of denial of service attackers. Large attacks may affect many thousands of devices, making manual recovery impractical. **Document References:** **Implementation Guidelines:** None	
PRODSEC27	**SEC-CHG-INTV**	**Maximum password lifetime**
	Condition: This requirement is **MANDATORY** for PRODUCTS that maintain their own password databases. **Requirement:** It **MUST** be possible to administratively specify that passwords, which have not been changed within a configurable interval, are to be automatically disabled. This interval **MUST** be administratively configurable over at least the range of one day to ten years, with a granularity of days. It **MUST** be possible to enable or disable this check on a per-user basis. The requirement may be satisfied either locally on the device, or in combination with an AAA server. **Status:** Current **Justification:** This is a step toward compliance with ANSI T1.276-2003 (M-53). **Document References:** **Implementation Guidelines:** It is extremely desirable to provide for warnings to users whose passwords are close to expiring.	
PRODSEC20	**SEC-CHG-PSWD**	**Authenticating at password changes**
	Condition: This requirement is **MANDATORY** for all PRODUCTS participating in password changes. **Requirement:** At any non-administrative password change, authentication using the old password **MUST**, by default, be required immediately before the new password is set. It is acceptable to permit administrative change to this behavior. **Status:** Current **Justification:** This is common security practice, and compliance is also a step toward compliance with ANSI T1.276-2003 (requirement M-15). **Document References:** **Implementation Guidelines:** The commonly used "Old password", "New password", "Repeat new password" dialog implements this.	
PRODSEC46	**SEC-CHG-LOGD**	**Changes to logging configuration always logged**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that support logging or auditing. **Requirement:**Whenever any form of logging is in operation, all changes to the configuration of the logging service itself **MUST** be logged in a reliable manner. For the purposes of this requirement, "changes to the configuration of the logging service" includes: • enabling or disabling logging, • changes in logging servers or other log data destinations, • changes to the logging protocols or to the configurations of those protocols, • changes in system wide logging filters, • changes to the logging severity or priority assigned to logging-related events such as loss of log data, • changes to the system's response to the exhaustion of logging resources, changes in the sizes of logging buffers, • other changes which might cause log entries to be lost, hidden, or misdirected.	

	Status: Current **Justification:** If the logging configuration can be changed without the change itself being recorded, the integrity of logs can easily be compromised. **Document References:** **Implementation Guidelines:** This is not meant to require the detection of changes to the stored logging configuration while the logging service itself is shut down.
PRODSEC13	**SEC-CHK-PUBL** — **Checksums published**
	Condition: This requirement is **MANDATORY** for all PRODUCTS supporting network-loadable software. **Requirement:** Hexadecimal SHA-1 or MD5 checksums for all released software files **MUST** be made available to customers. **Status:** Current **Justification:** Although the security provided is relatively weak, since there is no requirement that the checksums themselves be protected from modification, these checksums have been shown to be effective against some deliberate software modifications, as well as against many accidental corruptions. **Document References:** **Implementation Guidelines:** SHA-1 is considered best practice and it is recommended that there be a transition from MD5 to SHA-1 over time. For any products that are not providing a checksum now, it is recommended to start with providing SHA-1 checksums.
PRODSEC70	**SEC-CON-PERM** — **Connections permitted by source IP address**
	Condition: This requirement is **MANDATORY** for all STANDALONE DEVICES. **Requirement:** The STANDALONE DEVICE **MUST** have a capability to limit the permissible connections to any service on the device based on source IP address(es) of the connecting entity. **Status:** Current **Justification:** This feature allows access to the device to be restricted to known, trusted sources and expected traffic profiles. **Document References:** Opportunity Description Document For Baseline IOS Security Features **Implementation Guidelines:** "Receive ACL" feature as implemented on 12000
PRODSEC23	**SEC-CRE-REST** — **Password complexity restrictions**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that maintain its own password databases. **Requirement:**Any PRODUCT that supports creation of passwords **MUST** have the capability to enforce strong user passwords at the time of creation. At creation or any password change, the new password **MUST** be subject to all of the following restrictions as set by the administrator: • That the new password contains characters from at least three of the classes: lower case letters, upper case letters, digits, and special characters. • That no character in the new password be repeated more than three times consecutively. • That the new passwords not repeat or reverse the user name. • That the new password is not "cisco", "ocsic", or any variant obtained by

	changing the capitalization of letters therein. It **MUST** be possible to administratively disable each of these checks. It is acceptable to additionally provide a user interface for one-time overriding of these checks when a password is being changed administratively. The single exception is setting passwords for PRODUCTS that only support a numerical pin pad, which allows the digits 0 through 9, such as a telephone. The set of digits should be used for access to messaging services, and not for general computer networking services. **Status:Mandatory** **Justification:** This is a step toward compliance with ANSI T1.276-2003 (M-14). **Document References:** ANSI T1.276-2003 Baseline Security Requirements for the Management Plane; The Twenty Most Critical Internet Security Vulnerabilities, **The Experts' Consensus.** **Implementation Guidelines:**This requirement must be met by each product and not depend on an AAA server.
PRODSEC61	**SEC-CSA-INST-2** — **CSA preinstalled with capable Operating Systems**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that include an operating system capable of running the Cisco Security Agent (CSA). **Requirement:** CSA **MUST** be installed by default on each PRODUCT capable of using it. CSA **MUST** be preconfigured to permit any actions required by the installing Product, and to disallow any actions not required by that Product to at least the granularity of controlling file accesses in system directories and restricting network connections to expected services on a per-process or per-program basis. **Status:** Current **Justification:** CSA gives Cisco products a degree of immunity to operating system security problems, and even to their own security bugs. **Document References:** **Implementation Guidelines:** None
PRODSEC34	**SEC-DEF-CRED** — **No default authentication credentials**
	Condition: This requirement is **MANDATORY** for all PRODUCTS. **Requirement:** For all PRODUCTS there **MUST** be no authentication credentials which provide access to any protocol or service by default. Enabling a protocol or service **MUST** require the explicit definition of the credentials which are to be accepted for access to that protocol or service. The sole exception to this is at initial installation as provided in SEC-INT-CRED. It is not permissible to have any type of backdoor access (generally meaning an unacknowledged or undocumented access point) in a shipping PRODUCT. This means no backdoor passwords/credentials left for maintenance, TAC or development engineers. Authentication credentials include but are not limited to: passwords, shared keys, public keys, X.509 certificates, SNMP community strings and in some cases preset or permanent network addresses. **Status:Mandatory** **Justification:** Customers frequently forget to change default credentials leaving the devices at risk to any knowledgeable intruder. In some cases, customers may be unaware that default credentials exist at all. The security community tends to react vehemently to the discovery of any default credential, and to claim that the credential represents a deliberate back door; this can generate very negative press.

	Document References: SEC-INT-CRED permits unauthenticated configuration setup or the use of default authentication credentials at initial installation only, and specifies the conditions under which this can be done. **Implementation Guidelines**:Default credentials might include such things as default passwords or public keys accepted by default. In general, any password or key embedded in source code or in a default configuration file, even if encrypted and even if it can be disabled, is an example of a forbidden default credential.	
PRODSEC58	**SEC-DEV-ENCR**	**Encryption between devices**
	Condition: This requirement is **MANDATORY** for all STANDALONE DEVICES that include or are provided bundled with TCP/IP stacks or operating systems, whether those stacks or operating systems are developed by Cisco or obtained from third parties. The exception is for devices which are restricted to serving as single user, audio-only telephones, which have no functions not directly related to the establishment or maintenance of audio telephone conversations, and which do not participate in network protocols other than telephony protocols. **Requirement:** For layer 3 communications between Cisco STANDALONE DEVICES, encryption for confidentiality of user-selected traffic **MUST** be supported. IPsec ESP **MUST** be implemented by all STANDALONE DEVICES, except for devices which are restricted to serving as single user, audio-only telephones, which have no functions not directly related to the establishment or maintenance of audio telephone conversations, and which do not participate in network protocols other than telephony protocols. **Status:** Current **Justification:** Management traffic needs to be protected and user-selectable data may require confidentiality during transit. **Document References:** RFC-1851, The ESP Triple DES Transform; RFC-2403, The Use of HMAC-MD5-96 within ESP and AH; RFC-2406, IP Encapsulating Security Payload (ESP); RFC 2409, The Internet Key Exchange (IKE) **Implementation Guidelines:** To implement IPsec ESP refer to section 3.3.7 IPsec.	
PRODSEC1	**SEC-DOC-FEAT-2**	**Documenting required platform features and processes**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that use supporting software. **Requirement**: Any PRODUCT which uses supporting software, such as an operating system, database manager, or HTTP server, regardless of whether the software in question is developed by Cisco or provided by a third party, **MUST** document the essential set of features and processes which are associated with open ports of the supporting software which are used by the PRODUCT. For each feature, and process required by the PRODUCT the following MUST be documented: • The name, • Description of function, • Configuration information, • Any statically assigned TCP and UDP port numbers, • Use of dynamically assigned TCP and UDP port numbers and the range of these port numbers, • Traffic classification considerations (how is the traffic from the service recognized	

	for the purpose of filtering or applying QoS), • Any non-TCP and UDP protocols, • Any interdependencies with other features, applications and services. **Status:** Current **Justification:** This information is necessary to enable a thorough assessment of the security risks associated with the operation of the device, and to determine what steps should be taken to mitigate risk. One use of this information is for both Cisco employees and customers to understand what processes are running on a device, and to make decisions regarding security advisories and released security patches. **Document References:** ANSI T1.276-2003 Baseline Security Requirements for the Management Plane; ENG-83132, Serviceability Design Requirements for Security **Implementation Guidelines:** All applications, products or third-party software Cisco provides to a customer whom is running on a Windows, a Linux or other operating system that uses a database such as PostgreSQL, or uses an Apache web server, or other service needs to document these products' features and processes as defined above. **Note:** Be aware of the requirement, SEC-DEF-CRED, which states that no default authentication credentials are permitted. So when documenting a product, make sure there is no dependency on any default or static passwords/credentials. This also means no backdoor passwords left for maintenance or development engineers.	
PRODSEC11	**SEC-DOC-HARD-3**	**Hardening guides documented against**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that rely upon customer-supplied supporting software, such as operating systems, database managers, or HTTP servers. **Requirement:** If the vendor, SANS, or NSA has published a hardening guide for th user-supplied operating system software on which the Product relies, the Product's documentation **MUST** reference a specific version of that hardening guide, and ident any particular recommendations of that version which are incompatible with the Proc and/or give any product-specific information which users may need to implement the guide's recommendations. This implies that the product has to test on the hardened systems and document the recommendations in the release notes. **Status: Mandatory** **Justification:** Customers make heavy use of these guides, and need to know which recommendations will work with our products. Currently this is in compliance with the Security Initiative, phase 1. **Document References:** Examples on hardening guides from the vendors of operati systems and NSA website for Security Configuration Guides http://www.redhat.com/services/enterprisesecurity/securityhardening/ http://www.microsoft.com/technet/security/prodtech/windows2000/win2khg/de lt.mspx http://www.nsa.gov/snac/ **Implementation Guidelines:** It's almost certainly necessary to actually test on hard systems. PRODUCT documentation is also required to describe which system servic are actually required by the product, and the testing for the two requirements should easily combined.	

PRODSEC33	**SEC-DOC-RESET**	**Credential reset procedure documented**
	Condition: This requirement is **MANDATORY** for all STANDALONE DEVICES. **Requirement:** The process for resetting lost administrative credentials for STANDALONE DEVICES **MUST** be fully described in the customer documentation. **Status:** Current **Justification:** Customers need to know that password recovery is possible, and how it is done, so that they can properly secure against unauthorized password recovery. An undocumented procedure might be interpreted as a "back door", causing negative publicity for Cisco. In addition, documenting the procedure reduces support calls. **Document References**: **Implementation Guidelines:** None	
PRODSEC10	**SEC-DO-PSIRT-2**	**PSIRT contact required**
	Condition: This requirement is **MANDATORY** for all PRODUCTS **Requirement**: Each PRODUCT **MUST** have a designated contact from its BU to be listed as the contact for PSIRT issues. This contact will be used by the PSIRT when possible vulnerabilities are identified in the Product. In the case of products that incorporate 3rd party components, the responsible business unit contact **MUST** identify a corresponding contact with the 3rd party. **Status:Mandatory** **Justification:** PSIRT is the Product Security Incident Response Team. Their role is coordinating responses to discoveries of product vulnerabilities. They handle public communications as well as bug tracking. **Documentation References:** This requirement replaces, and is identical to, requirement CNEM00129 from the CNEM CTR, current version. **Implementation Guidelines:** 1. Go to the PSIRT contact database home page: https://wwwin-tools.cisco.com/Support/PSIRTVTS/prse/ExtViewStatusBoard.ps 2. Log in using your CEC username and password. 3. Select the Organizational Unit, then select the BU to update. 4. Click Go 5. A list will display, and you have the option to enter or edit the information. Note: Contact information contained in the previously used CAP database as of August 30, 2007 will be moved to the new PSIRT database.	
PRODSEC4	**SEC-DSP-PROC**	**Display of current running PRODUCT Processes**
	Condition: This requirement is **MANDATORY** for all PRODUCTS. **Requirement:** There **MUST** be a management interface that displays the processes which have open ports (often referred to as listening ports) being currently provided by the PRODUCT. This includes at least a list of processes, and for each process the following **MUST** be included: • The name, and • Addressing information (including ports). **Status:Mandatory** **Justification:** Customers want to know what processes are running on our products to understand the security implications. There have been cases where a security defect becomes known for a particular service or process, but one does not know if it applies to the product they are running. Also some processes may not be required and they may wish to turn them off. **Document References:**	

	Implementation Guidelines: An example is the output from the UNIX 'netstat' command.	
PRODSEC96	**SEC-FOR-ATTCK**	**Maintain forwarding during flooding attack**
	Condition: This requirement is **MANDATORY** for all FORWARDING DEVICES. **Requirement:** During any of the REFERENCE FLOODS, the FORWARDING DEVICE **MUST** maintain forwarding as follows: 1. Traffic sent through the FORWARDING DEVICE on any path not sharing interfaces with the REFERENCE FLOOD, at no less than 50 percent of the device's expected peak throughput. **Status:** Current **Justification:** Failure to maintain service creates obvious targets for attackers. **Document References:** **Implementation Guidelines:** None	
PRODSEC35	**SEC-INT-CRED**	**Initial configuration using default credentials**
	Condition: This requirement is **Optional** for all STANDALONE DEVICES. **Requirement:** As a special exception to other requirements in this document, a STANDALONE DEVICE**MAY** provide for unauthenticated configuration setup or for the use of default authentication credentials at initial installation only. If this is done, the STANDALONE DEVICE**MUST** have an initial configuration phase where it communicates with other devices on the same subnet or uses a "trusted" management port such as the console port. The initial configuration phase **MUST** include definition of required authentication credentials for further management or monitoring access, and **MUST** automatically disable all unauthenticated access and all default credentials. This requirement does not apply to and does not permit the use of null or default credentials by applications that are installed over general-purpose operating systems. Such applications **MUST** only allow initial configuration of authentication credentials during or after installation, using the "outside" facilities of the host operating system. **Status:** Current **Justification:** The only known way to configure a completely new device without permitting either unauthenticated access or the use of a default credential is to generate a specific initial credential for each device. This approach is logistically very difficult, and has security problems similar to those of the approach sanctioned in this requirement since secure delivery of the initial credential to the user is difficult. **Document References:** There is the example of AutoInstall using Serial Line ARP, which only communicates with another router using the same subnet address and uses either host address .1 or .2. Additional configurations of network devices by the customer are required for the router to get its initial configuration. Cisco Serial Line Encapsulation, EDCS-76024, 1/21/93; fr_autoinstall_cr_notes; http://wwwin-eng.cisco.com/ENG/IOS/WAN/SW_Unit_Functional_Specs/fr_autoinstall_cr-notes.txt; Dinnerbell IOS Deliverables for IAD platforms, ENG-79101. Another example is devices that have http web servers and only allow the administrator access via a web browser that is on the same subnet. Manufacturer's certificates are used in Cable modems today, and are being considered for other devices to provide initial identity or authentication. **Implementation Guidelines:** None	

PRODSEC63	**SEC-MGT-DEFT**	**Management protocol and service disabled by default**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that support configuration by other devices. **Requirement:** Except as described in SEC-INT-CRED, any protocol or service which permits a PRODUCT to be managed or reconfigured over a network, or which permits monitoring of or statistical data gathering from a PRODUCT over a network, **MUST** be disabled by default. **Status:Mandatory** **Justification:** Customers have frequently discovered that Cisco products have enabled management protocols of which the customers were unaware, and to which the customers had therefore applied no security protections. **Document References:** SSEC-INT-CRED permits unauthenticated configuration setup or the use of default authentication credentials at initial installation only, and specifies the conditions under which this can be done. **Implementation Guidelines:** None	
PRODSEC65	**SEC-MGT-ENCR**	**Management traffic encrypted for confidentiality**
	Condition: This requirement is **MANDATORY** for all remotely managed STANDALONE DEVICES or SYSTEMS that are managed as a single entity. In network management terminology that refers to a network element. **Requirement:** There **MUST** be a means to cryptographically guarantee the confidentiality of all data transmitted in protocols used for management, monitoring, or configuration. Ciphers and MACs used for these purposes **MUST** have 2^96 or greater work factors. **Status:** Current **Justification**: Integrity of management traffic is essential to the security of the managed network. Confidentiality of such traffic is of almost equal importance; management protocols frequently carry information which could be used to penetrate or disrupt the network. **Document References:** **Implementation Guidelines:** For TCP-based protocols, this is usually best achieved using TLS. For UDP-based protocols, it is usually best achieved using IPsec ESP or protocol-specific mechanisms. This document provides specific requirements for SNMP, terminal-mode CLI access, and HTTP; other protocols should be treated analogously.	
PRODSEC71	**SEC-MGT-FLOOD**	**Maintaining management during flood attack**
	Condition: This requirement is **MANDATORY** for all STANDALONE DEVICES. **Requirement:** If the STANDALONE DEVICE or SYSTEM has a connection path out of the path of the flood, the remote management connectivity to the device **MUST** stay intact even during any of the REFERENCE FLOODS. **Status:** Current **Justification:** Management functions are often particularly critical during attacks, since they are often the only means of characterizing or controlling the attack. **Document References:** **Implementation Guidelines:** None	
PRODSEC28	**SEC-NRCV-CRED-2**	**Hashing non-recoverable stored credentials**
	Condition: This requirement is **MANDATORY** for all PRODUCTS, which control the storage of their credentials. **Requirement:** Stored credentials, which do not need to be recoverable, such as inbound passwords, **MUST** be protected by a method at least as strong as an SHA-1 digest with a strongly random salt of at least 8 characters. **Status:Mandatory** **Justification:** Credentials stored in our products need to be protected against unintended exposure by using a strong cryptographic method.	

	Document References: ENG-83132 Serviceability Design Requirements for Security **Implementation Guidelines:** SHA-1, which is generally believed to be stronger than MD5, is the preferred cryptographic hash.	
PRODSEC12	**SEC-OPT-SIGN**	**Code signing optional**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that include bootstrap loaders, operating system kernels, or other dynamic loaders. **Requirement:** Software, which supports code-signing **MUST** support administrative configuration of the response to missing or invalid cryptographic signatures on the loaded software. At least the following two behaviors **MUST** be supported: 1. Halting of the software load process, with conspicuous reporting of the failure via all available user interfaces and logging services. 2. Loading of the suspect software, with conspicuous reporting of the failure via all available user interfaces and logging services. **Status:** Current **Justification:** Security-conscious administrators will want to prevent untrusted software from being loaded. However, there may be occasions on which it is necessary to run a patched image, or to run a corrupted image for long enough to permit installation of a new one. **Document References:** **Implementation Guidelines:** None	
PRODSEC31	**SEC-PHY-ACCS**	**Physical access required to reset lost credentials**
	Condition: This requirement is **MANDATORY** for all STANDALONE DEVICES. **Requirement:** The process for resetting lost administrative credentials for STANDALONE DEVICES **MUST** involve some action which can, as far as can be determined by the device, be performed only by a person with immediate physical access to the device being recovered. **Status:** Current **Justification:** Without software credentials, physical access to the device is the only even slightly reliable way of verifying ownership. Furthermore, since Cisco devices do not in general protect themselves against physical disassembly, permitting a person with physical access to recover software access creates a reasonably limited additional security exposure. **Document References:** Cisco IOS Security Configuration Guide, SC-431 **Implementation Guidelines**: Cisco IOS has traditionally implemented this requirement by attempting to require the user to demonstrate the ability to power-cycle the device. This is an acceptable method, but it can be difficult to be sure that there has been a real power cycle as opposed to a software event. Furthermore, customers occasionally want to permit remote control over the power for their equipment. It is best to implement this requirement using a dedicated recovery switch on the device chassis.	
PRODSEC9	**SEC-PRT-TAB-2**	**Management port labels**
	Condition: This requirement is **MANDATORY** for all STANDALONE DEVICES. **Requirement:** If a STANDALONE DEVICE has an external, physical management port such as a console port or a dedicated management LAN port, and if the software in use allows greater control over the device from the management port than from other ports on the device, then that port **MUST** be prominently labeled in such a way that the label will be read by anyone physically installing the device. The label of a serial port as a "console port" is deemed sufficient to meet this requirement. The labeling of a network port can use the text "network management port" or "netwk mgt" to meet this requirement.	

	Status: Current **Justification:** There has in the past been customer confusion over these ports. **Document References:** Product Security Design Requirements ENG-83132 **Implementation Guidelines:** None	
PRODSEC8	**SEC-SET-TIME**	**Set and maintain accurate time**
	Condition: This requirement is **MANDATORY** for all STANDALONE DEVICES. **Requirement:** Each STANDALONE DEVICE **MUST** have a mechanism to set accurate time on the device, and to maintain it within 500 milliseconds of actual clock time. Unless some essential function of the device requires it to participate in another protocol which provides accurate time, or requires the device to measure time directly, the device **MUST** support the use of Network Time Protocol, NTP version 3 as specified in RFC 1305, for this purpose. **Status:Mandatory** **Justification:** Audit records must include the date and time. To correlate events across a network, the time stamps on the audit records need consistent and accurate times. **Document References:** ANSI T1.276-2003 Baseline Security Requirements for the Management Plane **Implementation Guidelines:** None	
PRODSEC74	**SEC-SSH-V2.0**	**Support for SSH v2**
	Condition: This requirement is **MANDATORY** for all PRODUCTS that support text-mode user interaction from a network connection. **Requirement:** Any PRODUCT which supports text-mode user interaction from a network connection **MUST** support such interaction via the SSH version 2 protocol. **Status:Mandatory** **Justification:** SSH has emerged as a de facto industry standard for secure text-based logins, and is available for essentially every major OS platform. Many security-conscious customers want to use SSH to manage all their equipment. SSH is a key element of Cisco's protocol suite for interoperability. There is the belief that SSH should be part of the base level component of any operating system that Cisco is supplying the customer. **Document References:** **Implementation Guidelines:** There is no requirement for SSH version 1 support, but some customers may still ask for it. Writers of PRDs are advised to consider it. When implementing, the common version of SSH to test against is OpenSSH. SSH uses a public/private key pair to identify the server. This key pair must be stored locally. The private key is very sensitive, and must be protected. Compromise of the private key would allow an attacker to both interlope and potentially pose as the host itself.	
PRODSEC18	**SEC-SUP-CHAR**	**Supporting minimal character set in passwords**
	Condition: This requirement is **MANDATORY** for all PRODUCTS processing passwords. **Requirement:** Any struck character from the ASCII character set **MUST** be supported in passwords. The struck ASCII characters are as follows: !"#$%&'()*+,-./ 0123456789 :;<=>?@ ABCDEFGHIJKLMNOPQRSTUVWXYZ [\]^_` abcdefghijklmnopqrstuvwxyz {|}~	

	This is not to be construed as forbidding support for additional characters. **Status:** Current **Justification:** The struck ASCII set is universally available and easily parseable by CLIs and scripting tools. By ensuring that all of Cisco's products can accept at least all of these characters, this gives users a reasonably broad choice of characters for passwords which can be used on multiple devices. **Document References:** **Implementation Guidelines:** This is a minimum requirement. Many new products may support entering passwords containing any Unicode character. However, this can introduce problems, because Unicode comparisons can be difficult.
PRODSEC110	**SEC-SUP-PATCH** — **Ability to support security patch process**
	Condition: This requirement is **MANDATORY** for all THIRD-PARTY SOFTWARE. **Requirement:** There **MUST** be a process in place in which security patches and fixes to bundled THIRD-PARTY SOFTWARE are propagated into the PRODUCT including the installed base. **Status:** Current **Justification:** Customers cannot be asked to run software that is at risk, or prevented from applying security patches due to compatibility concerns. In addition, customers may not even be aware of the existence of third-party software bundled with Cisco products, and will expect Cisco to provide appropriate protection. Mass worms such as Code Red and Nimda have highlighted the necessity of keeping up to date with security fixes and patches. **Document References:** http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml, http://www.cert.org/advisories/CA-2001-23.html **Implementation Guidelines:** None
PRODSEC73	**SEC-VER-INFO** — **Restrict version information**
	Condition: This requirement is **MANDATORY** for all PRODUCTS. **Requirement:** The implementation name or version information provided by any PRODUCT to its peer in any network protocol **MUST**, by default, be limited to the information actually required for the protocol to work properly given a standards-conformant peer. If a protocol field for implementation information is optional, it **MUST** be omitted entirely. If the protocol field is MANDATORY, but its contents are left to the implementer's discretion, then any name field **MUST** if possible, be filled in with a null string. If a null string is not acceptable under the protocol specification, the string "unspecified" may be used. Any version field **MUST** be filled in with "1.0", or if the field is purely numeric, "1". The sole exception to this requirement is when accurate implementation version information is absolutely required by an externally imposed industry standard. **Status:** Current **Justification:** Implementation information may allow peers to identify vulnerable software. Modifying protocol behavior based on the implementation version of a peer is at best an architecturally questionable practice so depriving communication devices of this information should not present an undue hardship. **Document References:** http://www.securityfocus.com/infocus/1612. **Implementation Guidelines:** Note that this does not apply to fields identifying the versions of protocols, but only to fields identifying particular implementations. For example, in the HTTP protocol, the client sends protocol version information in the first line of the exchange, as in "GET /foo.html HTTP/1.1"; this information is not affected by this requirement. On the other hand, HTTP's "User-agent" field is implementation information, and should not, by default, be sent by any Cisco client. For the specific case of HTTP, it may be desirable to permit the user to override this default, and to specify a string of his/her choice for the "User-agent" field.

CA Requirements in the High Availability Baseline

High Availability Baseline requirement document EDCS-575733

All technical questions regarding High Availability requirements should be sent to ha-baseline-alias

ReqProID	Requirement Name	Requirement
HA479	**Troubleshooting Guides**	The development team **MUST** schedule time in the project schedule to write troubleshooting guides for commonly expected field failures. Reference • SWSW Trouble Shooting Guide : Release 9.3, ENG-76904; http://wwwin-eng.cisco.com/Eng/WAN/Switch_SW/TSG/93_TSG/book/WEB/tsgTOC.fm.htm Increasing Network Availability with ECC; http://www-tac/Support_Library/Hardware/ECC/ecc.html

CA Requirements For Daylight Savings Time

The setting and maintaining of accurate time is a key requirement for all customers. The accuracy of date and time allow customers to accurately correlate events across a network based on the date and time in the audit records.

Daylight Savings Time and Time Zone Dashboard –
http://www-tac.cisco.com/Support_Library/Products/Cisco_Products/Voice_and_Unified_Communications/Voice_Applications/Dashboard_for_Daylight_Savings_Time.html

Found in **EDCS-626045**

(Formerly CA DST Requirements)

ReqProID	Requirement Name	Requirement
CNEM-dstz-01001		**Status** Current **NM Function** Provisioning **Requirement Condition** Conditional Mandatory **Specific Requirement** Products MUST support IEEE-1003.1-2004 (POSIX) TZ strings for timezone information. **Condition Details** This requirement is applicable to all products that are not based on Windows and products that are based on Windows but do not use the host operating system's timezone.

		Implementation Guidance Any modern UNIX-based system should already support this standard. For those systems that do not, free code is available from elsie.nci.nih.gov. To convert a TZ (Olson) Database string to a valid POSIX TZ string, code is available from http://wwwin-cons.cisco.com/~elear/n2p.tgz. While user interfaces can provide for more human friendly versions of this string, the underlying product should never the less be capable of understanding the actual string, so as to ease its distribution from a central management source. **Rationale** The POSIX TZ string provides a flexible means to specify timezone definitions. By specifying the actual definitions it is possible for customers to update their timezone definitions without having to update an entire timezone database, as may not be possible in some environments.
CNEM-dstz-01002		**Status** Current **NM Function** Provisioning **Requirement Condition** Conditional Mandatory **Specific Requirement** Products MUST make use of the TZ (Olson) timezone database, and provide in their administrative interface an input method for the TZ names specified there-in. **Condition Details** This requirement is applicable to all products that are not based on Windows and products that are based on Windows but do not use the host operating system's timezone. **Implementation Guidance** Code is freely available from elsie.nci.nih.gov. The code is POSIX compliant. **Rationale** The mnemonics used by this database are nearly universal. Their use provides an easy way for customers to consistently implement timezones across their network without having to specify actual definitions. **Notes**
CNEM-dstz-01003		**Status** Current **NM Function** Provisioning **Requirement Condition** Conditional Mandatory **Specific Requirement** Products MUST implement the DHCP Timezone options as specified in RFC-4833; specifically, the two options for DHCPv4 and the two options for DHCPv6. **Condition Details** Applicable to all non-Windows network elements that implement the DHCP client interface. **Implementation Guidance** ISC DHCP client code includes a contrib. entry that supports the TZ name option. **Rationale** Centrally managed, DHCP can provide a standard approach to deliver timezone information to clients. **Notes**
CNEM-dstz-		**Status** Current **NM Function** Provisioning **Requirement Condition** Conditional Mandatory

01004		**Specific Requirement** Products MUST implement a mechanism to update local list of timezone definitions, change configured timezone, and/or change configured DST settings without requiring service interruption. **Condition Details** Applicable to ALL Windows-based products and all other products that are unable for whatever reason to implement the other requirements above. **Implementation Guidance** Most releases store this information in the Windows registry. See http://msdn.microsoft.com/library/en-us/sysinfo/base/time_zone_information_str.asp for details. **Rationale** Windows has its own database and registry mechanism to update timezones. This may vary from release to release. It is the responsibility of the product group to see that there is a mechanism included with their products to update these definitions. **Notes** In future it would be nice to have some code to hand out.
CNEM-dstz-01005		**Status** Current **NM Function** Provisioning **Requirement Condition** Conditional Mandatory **Specific Requirement** Products MUST provide an administrative interface to set or change defaults and to store these settings persistently without service interruption: · Timezone Setting · Enable or Disable DST · Recurring DST Start Date & Time · Recurring DST End Date & Time **Requirement Condition Details** Applicable to ALL products which uses TZ information and/or acts as a TZ reference source for other products.

3.13 [redacted] Automation SKUs

The [redacted] Automation switches have the following unique characteristics from the Cisco version of the switch:

1. [redacted] Automation color scheme - to be defined
2. Product Face Plate – including [redacted] branding and Cisco technology logos onthe exterior of the switch.
3. Product Label – Unique product label – to be defined
4. Device Manager - Unique look and feel per [redacted] Automation style guide. Device Manager content is not unique. Please refer to Exhibit B in the Co-Branded Technology Solution Agreement.

5. MAC ID - The [redacted] Automation switches use MAC addresses from [redacted] address space. The Cisco switches use MACaddresses from Cisco's address space.Please refer to Exhibit B in the Co-Branded Technology Solution Agreement.
6. [redacted] Automation IDs – This includes unique product identifiers as represented in the CIP interface, Device Manager and CLI. For example the CLI 'show version' command output does not change anything with respect to the [redacted] switch, except to display the different product IDs and SKU brand name (Cisco or [redacted]. Also the [redacted] Automation switch is supported in RSLogix 5000 for configuration and enhanced support of the I/O connections. Please refer to Exhibit B in the Co-Branded Technology Solution Agreement.
7. Default switch configuration - The [redacted] Automation switch has a unique requirement on default configuration. [redacted] supports this functionality through a [redacted] Global Smartport template. The switch uses the Cisco default configuration file when it comes up for the first time and behaves as an un-managed switch. Express Setup then applies the optimized configuration by running the [redacted] Global Smartport template. The configuration changes are written to the configuration file. When customers erase the configuration (write erase) and reload the switch, the switch comes up with the Cisco default configuration for an un-managed switch. The [redacted] Global Smartport template does not contain any [redacted] specific features, but configures features that optimize switch operation for use in industrial applications. Please refer to Exhibit B in the Co-Branded Technology Solution Agreement.
8. LED functions - The [redacted] Automation switches have unique LED functions per section 2.2.4.6.
9. Smartports - The [redacted] Automation switches contain unique Smartport macros for specific EtherNet/IP applications. Each smartport includes three components: an icon, a name and a configuration. The Ciscoswitches do not contain macros for specific EtherNet/IP applications, but instead have a generic macro for allEtherNet/IP compliant devices. Please refer to Exhibit B in the Co-Branded Technology Solution Agreement.

4 Internal Specifications

4.1 Overview

Primary components are CPU, memory, switch ASIC, and Ethernet PHYs.

4.2 Major Components

This section gives a brief overview of [redacted] hardware:

Yeti3:. It is a low cost system controller based on the PowerPC 405 RISC core, which provides control and management functions through MIC interface which allows for control of the port

ASICS. Also, it provides a 16-bit External Bus Controller (EBC) interface that performs control and monitoring of different slave devices such as flash memory. Yeti3 supports DDR2 DRAM.

DDR2- SDRAM: Design supports 128MB of DRAM. The DRAM will be used for storing the IOS runtime binary image and for all dynamic memory allocation requirements (including IO memory).

Flash: Design supports 64MB flash part. There is one flash footprint which will support both Spansion and Nymonnyx/Intel flash memories.

Console:UART interface to CPU used for switch management functions.

Sparkplug FPGA: Needed for SD Flash support.Using Xilinx XC3S200AN FPGA.

FECR: A multi-port Ethernet network interface to the HULC stacking system. This ASIC is sourced from ST Microelectronics using a 580 pin EPBGA, 35mm^2, 1.0mm pitch. The FECR terminates 24 FE ports (SMII) and 2 GE ports (SGMII), interfaces with Yeti3 (HULC Supervisor), hosts a TCAM2 and an SRAM integrated into the device. In this usage there is no external HULC interface.

Jeeves FPGA: Only used on Stretch PCB, adds 1588/NAT and expansion port functionality. Using Altera EP2AGX FPGA.

BCM5248 PHY: Octal Fast Ethernet PHY supports 10/100Base-T/TX operation or 100Base-X operation.

FE Magnetics: The magnetics provide the required isolation between the DAC of the PHY and the CAT5 transmission lines. Integrated connectors and magnetics, or MagJacks, are not proposed for this architecture as an isolation circuit must be introduced between the connector and magnetics to protect against high levels of transient power Camaro. The electrical characteristics are in compliance with 10BaseT and 100BaseTX.

BCM5482 PHY: Dual Gig Ethernet PHY supports 10/100/1000Base-T/TX operation or 100/1000Base-X operation.

GE Magnetics: The magnetics provide the required isolation between the DAC of the PHY and the CAT5 transmission line. The electrical characteristics are in compliance with 10BaseT, 100BaseTX, and 1000BaseTX (IEEE 802.3ab).

Temperature Sensor: It is an I2C temperature sensor device used to report ambient temperature inside chassis for informational and alarm purposes.

Quack2:A security chip, used to store unit specific data to prevent counterfeiting of Cisco products.

Alarm I/O: All sku's support adry contact alarm output connector, with a common, normally open and normally closed terminals. Also has two dry contact alarm inputs, where a circuit open or closed state is detected. Alarm in can be set for either a normally open or normally closed condition.

4.2.1 Software

The following SW components will be changed/added for [redacted]

4.2.1.1 Boot Loader

To reduce the boot time for Camaro, the following actions are considered:

a. IOS image compression will be changed from BZIP2 to CZIP
b. Disable POST
c. Disable memory test (RAM)
d. Disable extensive FSCK test

Items b-d will be configurable via the IOS boot command.

4.2.1.2 Licensing Model

Camaro will leverage licensing model from previous projects such as pixar to provide one single image that can support either IA Lite or IA Base. There will be two regions reserved in on-board flash for this feature.

4.2.1.3 Diagnostics

Camaro will provide an additional link status parameter for signal strength indication. The new parameter will be reported as part of the ongoing link monitoring/status.

4.2.1.4 Removable SD Flash

A new software component will be added to handle the appropriate actions when the SD card is present in the Camaro system. For more detail, please refer to [redacted] SW FS.

4.2.1.5 IEEE 1588

This feature enhancement will be implemented in the Jeeves FPGA and the associated IOS software. For more detail, please refer to Jeeves FPGA ERS and [redacted] SW FS.

4.2.1.6 NAT

This new feature will be implemented in both Jeeves FPGA and IOS software. The division of address translation work between the FPGA and IOS depends on the complexity of the protocol fixups. Simple protocol fixups such as the IGMP will be handled by the FPGA. Otherwise, the FPGA will "punt" the packet to the CPU for further processing. The communication path between the FPGA and the CPU is shown in the HW section 2.2.3, in particular, the system block diagram "Stretch". For more detail, please refer to Jeeves FPGA ERS and Camaro NAT FS.

4.2.1.7 Jeeves FPGA upgrade

To support the FPGA image upgrade, the [redacted] software will need to copy the new image to the on-board flash via the MIC Ring. For more detail, please refer to Jeeves FPGA ERS and Camaro SW FS.

4.2.1.8 Network Management

NMS team's input

4.2.1.9 MIB

Both CISCO-NAT-EXT-MIB and CISCO-IETF-NAT-MIBare used to include NAT monitoring parameters. Please note that not all objects will be supported in [redacted]. For more detail, please refer to Camaro SW FS.

4.2.1.10 CIP

The CIP enhancement features will be added on the existing CIP stack. Some enhancement feature require new CIP objects which have their own classes. Some enhancement will use new attributes in the existing CIP objects.

4.3 Major Data Structures

In Camaro, the IOS image will use CZIP compression to reduce boot-up time. Furthermore, the SD flash card will utilize the FAT FS to support the PC readable format requirement.

4.3.1 [redacted] Specific IDs stored in flash

The Camaro switches have the following numbers stored in FLASH during manufacturing cycle and used by IOS SW.

- Cisco Switch Serial No (on both Cisco and Rockwell switches)
- CIP Serial No
- Mac Address
- Module EEPROM parameter

4.3.1.1 Switch Serial Number

Cisco branded switch. Uses 11 bytes serial number generated by Cisco manufacturing process as per Cisco formatgiven below:
CMCode (3 bytes) - Year (2 bytes) - Week (2 bytes)- CM ProductionLine (1 byte) - number (3 bytes of base34 number).

Both CLI command - 'show version' and device manager display this number as 'Switch Serial No'.

Rockwell Automation branded switch. Also has Cisco Serial Number in the flash, however, only CLI command - 'show version'displays 11 byte Cisco Serial Number as 'Cisco Serial No'. The Device Manager does not display Cisco Serial Numberbut does use CIP Serial Number to display [redacted] Switch Serial No' (see below).

4.3.1.2 CIP Serial Number

The CIP Serial Number is unique for each switch unit under the same Vendor ID and is used by CIP software modulein IOS. The size of this attribute is 4 bytes as defined by CIP standard.

Cisco branded switch. Derives 32 bits CIP Serial Number from the switch default MAC address of 48 bits. Sincethe manufacturing team keeps track of MAC addresses assigned to Cisco products, these same automated scripts pickunique 32 bit numbers for the CIP Serial Number.

The automated scripts map the lower 24 bits of CIP Serial number equal to NIC part (24 bits) of MAC address. Theautomated scripts keep track of OUI currently used for Xmen2 switches and maintain a table mapping OUI to theremaining 8 bits of CIP Serial Number. In short, CIP Serial Number (32 bits) comprises 8 bits of mapped OUI and 24bits of NIC.

[redacted] **branded switch.** Uses a block of CIP Serial Numbers provided by [redacted] It is stored in the FLASH asper the CIP specification in hex. The manufacturing team just pulls a number from the list and writes into flash. It ishuman readable on the PID (Product ID Label). It is optional to have this on the PID as a bar code as well.

The output of a CIP CLI command to show the attributes of Identity object contains the CIP Serial Number. TheDevice Manager uses this CIP Serial Number to display as [redacted] Switch Serial No'.

4.3.1.3 MAC Addresses

Cisco branded switch. The MAC addresses are assigned from Cisco MAC address pool.

[redacted] **Automation branded switch.** The Cisco manufacturing tool assigns the MAC addresses from the MAC address poolprovided by [redacted] Automation. MAC addresses provided by [redacted] are integrated into Cisco MARS (MAC Address Replenishment System). [redacted] supplies 6 - 12 months worth of MAC addresses. It is human readable on the PID(Product ID label). It is optional to have this on the PID as a bar code as well.

4.3.1.4 ID that differentiates the [redacted] and Cisco switches

The ID field 'MAKE' from EEPROM fields differentiates if the switch is Cisco branded or [redacted] branded. TheIOS SW reads it and exposes the identity to other modules including Device Manager.

4.3.1.5 Summary

Parameters/IDs	Cisco branded	Rockwell Automation branded
Switch Serial No	Standard 11 byte number generated by Cisco manufacturing tool. The CLI command 'show version' displays it as 'Switch	[redacted] brand also has 11 byte Cisco serial No in the flash. The CLI command 'show version' displays it as 'Switch

	Serial No'	Serial No', however, the Device Manager does NOT display it as 'Switch Serial No'. Instead, it uses CIP Serial Number to display as '[redacted] Switch Serial No'
CIP Serial No	Cisco manufacturing tool uses a new script that derives this 4 bytes number from switch base MAC address and stores in flash. Only used by CIP SW module.	Provided by [redacted] and stored in the flash by Cisco manufacturing tool. The output of a CIP CLI command to show the attributes of Identity object containing the CIP Serial Number. The Device Manager uses this CIP serial Number to display as [redacted] Switch Serial No'.
MAKE ID in EEPROM fields	Unique value for Cisco. Used by IOS SW and Device Manager to differentiate the switch brand	Unique value for [redacted] Used by IOS SW and Device Manager to differentiate the switch brand.
Mac addresses	Assigned from the Cisco MAC address pool.	Assigned from the [redacted] MAC address pool.

4.4 Major External Interfaces

The new CIP enhancements will have new CIP objects and new attributes in the existing CIP objects.

4.5 Major Internal Interfaces

The only major internal interface in Camaro is the communication path between the Jeeves FPGA and the CPU. Please refer to section 4.2.1.5 – 4.2.1.7 for more detail.

4.6 Software Memory Estimates

Most L2 functionalities will be leveraged from the existing platform IE3K, memory utilization will be the same as of IE3K platform. The SW memory estimate is taken from IE3K (ies-lanbase-mz). [redacted] will support two SDM templates: default and dual-ipv4-ipv6-default as in IE3K.

Table 4.1: Software Memory Estimates

S/W Feature	Baseline Estimate	Current Estimate
IOS LANBASE image	8M	
SDRAM	13M	

4.7 Hardware Memory Options

The hardware design will be designed to support multiple sizes of memory for flexibility and future upgradability if required. However, the plan of record will for all skus to ship with 32MB of flash and 128MB of SDRAM.

Table 4.2: Hardware Memory Options

Memory	Min	Max
Flash (onboard)	32MB	64MB
SDRAM (main)	128MB	512MB
SD Flash		1GB

4.8 Performance

Performance goals include:

1. 1588 time stamp insertion at port line speed, latency and jitter not to exceed performance of Xmen2.
2. Ability to do NAT translations at wirespeed (<5 micro second delay.)
3. NAT translation jitter between first entry and last entry in the table should be <30 micro seconds.
4. Per flow NAT translation jitter should be <20 micro seconds.
5. System boot time from power apply to IOS operational not to exceed 60 sec (goal is 30 sec).

5 Issues, Risks and Dependencies

5.1 Platform Requirements

5.1.1 Cisco PID

Currently, there are two different Cisco PIDs for each [redacted] labeled switch. For example, the IE-2000-4TS-L and IE-2000-4TS-B indicate the same box with different IOS images. When [redacted] software has the software license upgrade capability, the IE-2000-4TS-L box can have the IA Base image. However, the Cisco PID is still –L. This may be a violation as far as Cisco PID is concerned.

5.2 Related Projects

TMG will need to develop/productize SFPs to be supported in the hardened sku (IE-2000-16TC-G-X.) These SFPs will need to meet similar specs as laid out in section 3.14

We will work with TMG to try to develop the following SFPS:

GLC-FE-100FX

GLC-SX
GLC-LH
GLC-FE-100LX
GLC-ZX
GLC-EX

Availability will depend on finding third party SFP suppliers willing and able to develop each of these.

5.3 Third Party Relationships

Half of the [redacted] SKUs are for 3rd party, [redacted] Automation. They will have different front panel overlays with different color scheme, text, and logo.

There is no new third party software introduced in [redacted] project. The existing Softing (Profinet source code) relationship had been established for IE3K project.

5.4 Sole / Single Source Components

Sole Source Components

Most ASICs on [redacted] are sole source components. Additional sources are not available at this time. These include Yeti-3, FECR and PHYs such as BCM5248, and BCM52482. In addition to these ASICs, the FPGA, CPLD, PSoC MCU, and PWM controller devices for DC/DC converters will also be sole source components.

Single Source Components

Where available, multiple sources will be qualified during the [redacted] P1b and P2 builds. A list of the 2nd source qualification plan will be found in the "AVL Build Matrix". The matrix will be loaded into EDCS prior to the P1a and P2 builds.

5.5 Technology Requirements

The only new technology that will be required is to work with the contract manufacturer to develop the ability to conformal coat skus. Our current CM's traditionally do not conformal coat products for Cisco. We are engaging with the Cisco manufacturing team and the contract manufacturers to develop the best strategy for achieving this requirement.

5.6 Technical Risks

Table 5.1 - Technical Risk Management Plan

No.	Risk/Impact Description	Prob	Impact	Risk Management Strategy

5.6.1	IOS boot-up time **Risk**: exceeds 30sec **Impact**:Marketing (customer)	High	Medium	**Abatement** – Testing on IE3K and IE3010 platforms indicates that desirable 30s target cannot be hit but <60s should be possible **Mitigation** –In the event that the boot time extends past the 60s boundary additional feature removal could help mitigate **Contingency** – A different HW architecture would help address the requirement but would drastically change the scope of the program
5.6.2	Risk/Impact Description Name **Risk**: **Impact**:	Low	High	**Abatement** – **Mitigation** – **Contingency** –
5.6.3	Risk/Impact Description Name **Risk**: **Impact**:	Low	High	**Abatement** – **Mitigation** – **Contingency** –

6 Requirements Traceability Considerations

TL 9000 is not a requirement for [redacted] (IE2K/S7K)per section 15 in the PRD, so traceability is not applicable.

7 References

- [redacted] External PRD, EDCS-869395
- [redacted] SW Functional Spec, EDCS-964004
- [redacted] CIP Functional Spec, EDCS-920154
- [redacted] NAT SW Functional Specification, EDCS-974591
- Xmen2 System Functional Specification, EDCS-480000

End of Document