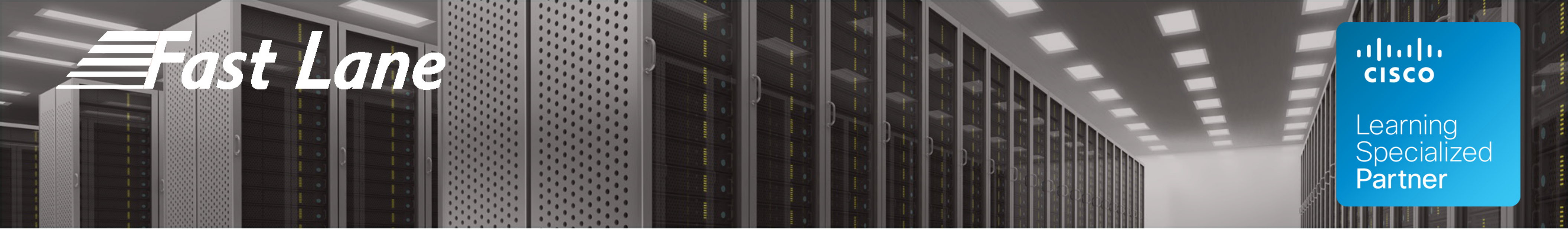


CUSTOM SDA MENTORED INSTALL (SDA-CUST-MI)

A variable day Production Network SDA Mentored Install covering policy adoption with compliance services such as Identity Services Engine (ISE) and Stealthwatch that are determined based on the needed scope of the organization. The mentored install covers DNA-C and ISE Implementation. FL SMEs work alongside Customers to deploy ISE, integrate ISE with existing Active Directory, set up ISE Management Access, and create necessary users and end-user portals. The final step in the Mentored Install service is to test and validate the agreed upon Use Cases and test plan, as well as an Assurance Review, in which FL SMEs verify Assurance is collecting analytical information. Integrations with other products including but not limited to, Cisco FirePower, Cisco Web Security Appliances (WSA), etc., can be included at an additional cost to be determined after the scope discovery process.

Prior to scheduling the mentored install, FL SME and team work with Customers to agree on specific Use Case(s) and create a High-Level Design Document (HLDD) for the Use Case(s). The HLDD operates as the road map for the Mentored Install.

PRICING

Pricing is based on project objectives and requirements

Pricing includes Mandatory Discovery/ Planning Workshop and DNAC.

FAST LANE SDA MENTORED INSTALL SERVICES

Fast Lane is a Global Consulting and Education Services company with a focus on Cisco, Microsoft, NetApp, Gigamon, Barracuda and others. Fast Lane provides Professional Services that augment and support our vendor partners and their partner ecosystems.

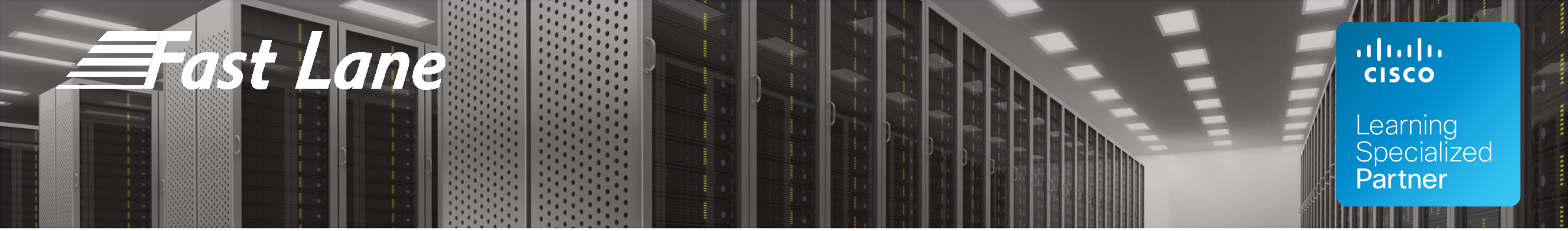
Fast Lane (FL) offers Mentored Installs, Expert for Hire (E4H) Sales enablement consultancy solutions, Digital Transformation services, Learning-as-a-Service platform services along with authorized vendor training solutions.

Fast Lane is pleased to propose a Mentored Install of Cisco® Software-Defined Access (SD-Access), the next-generation architecture for the enterprise network. Aligned with the Cisco Digital Network Architecture (Cisco DNA™), also offered by Fast Lane, SD-Access uses a centralized controller to provide a management framework. This framework will simplify the provisioning of your network, administer group-based policy for users and provide telemetry to help identify problems and provide corrective actions. The proposed Cisco SD-Access provides a cohesive, end-to-end security architecture that addresses the unique needs of the customer while conforming to the latest industry trends. This solution's automation and simplicity will allow IT professionals more time to innovate, while also helping them initiate network changes more rapidly and efficiently. Scalable virtualization capabilities in the infrastructure help create hierarchical micro/macro segmentation policies that are enforced with the fabric infrastructure for secure segmentation. Thanks to its long-term cost reduction, centralized management, on-demand provisioning, and network flexibility, the proposed Cisco SD-Access provides operational and strategic advantages over traditional enterprise networks.

The proposed solution transforms the network from a vendor proprietary system to an open and programmable infrastructure. Rather than dealing with disparate networks and setting up multiple VLANs, it automates many processes and supports virtualization. With the proposed Cisco SD-Access you can simplify your enterprise campus, WAN, and branch environments, increase network security and scale network resources with your application and data needs.

There are multiple types of engagements available ranging from Isolated Mentored Install Deployments with various onsite days to Production Network Integration Deployments.

Engagements begin with our one-day offering and can extend longer depending on the services required. Each engagement will be scoped by a Fast Lane Subject Matter Expert and team and a detailed Statement of Work (SOW) will be created for the type of engagement.



DISCOVERY PLANNING WORKSHOP

Fast Lane consults with the partner and customer engineers in order to establish the required Use-Cases and complete a High-Level Design Document (HLDD). The actual scope of the engagement determines the tier level of detail workshop. Discussions include:

1. Business Objectives
2. Business Timelines
3. Collection and validation of network diagrams (Physical and Logical), campus floor and area layouts, and site information. (Out of date or incomplete documentation will need to be made current and validated prior to planning/design sessions)
4. Endpoint grouping information (Employee, Contractor, Printer/Scanner, Camera, Servers, etc.).
5. Existing network services information (AAA, DHCP, DNS, NTP, Logging, etc.).
6. Existing network device inventory and device information (to be used in the network readiness assessment).
7. Identity Store Details (Microsoft Active Directory, LDAP)
    - 7.1. Verify Active Directory/LDAP configuration and health
    - 7.2. Evaluate any Forest and/or Domain Trust configurations
8. ISE Deployment Details:
    - 8.1. Verify ISE VM performance minimum requirements
    - 8.2. Document existing ISE deployment including:
        - 8.2.1. Network Devices and Configuration
        - 8.2.2. Network Access Policies
        - 8.2.3. TrustSec Configuration and Policies
        - 8.2.4. Network Device Admin Policies
9. Operations
    - 9.1. High Availability and Redundancy Requirements
    - 9.2. Security Policy Requirements
    - 9.3. Application Node Details
    - 9.4. PKI/Certificate Infrastructure Configuration, Operations and Health
    - 9.5. Help-Desk Workflows
    - 9.6. Security Operation Workflows
    - 9.7. Migration Requirements
    - 9.8. Backup Repositories and Requirements
    - 9.9. Reporting Requirements
    - 9.10. Outstanding Environment Troubleshooting or Remediation Needs
10. Determine Performance Requirement Specifications
11. Design Session(s) with Resource Team
    - 11.1 Review Existing Environment
    - 11.2 Evaluate requirements for implementation of SD-Access into a green-field or brown-field environment based on verified Use Cases.
12. Determin basic security enforcement policies based on agreed upon Use Cases
13. Develop Build of Materials (BOM).

CUSTOMER RESPONSIBILITIES

•Participate in Preliminary Discovery Sessions(s) via Cisco Spark or Cisco WebEx.
•Participate in High Level Design Session(s) via Cisco Spark or Cisco WebEx.
•Provide a solution success verification plan.
•Provide a proper environment for the deployment. Including, rack space, cabling, conditioned power, heating/cooling, etc.
•Update environment to recommended software/firmware versions prior to FL-SME arriving onsite.
•Provide actual software.
•Rack and verify equipment prior to FL SME arrival.
•Provide adequate resources to perform the implementation with FL SME while FL SME provides interactive training and coaching.
•Aid in all testing scenarios (either from Partner Resource Team and/or Customer Resource Team).
•Provide updates regarding any Move/Add/Changes to the environment during the scope of the engagement.

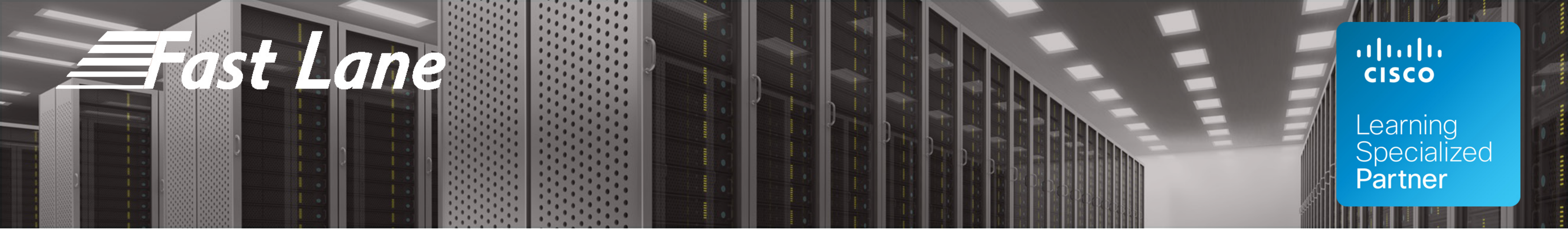
STATEMENT OF WORK

After the FL SME completes the Mandatory Discovery and Planning Workshop and produces the HLDD the FL Product Manager will prepare the proposal, SOW and Project Plan based on the client's acceptance of the proposal.

TRAINING

Supplemental training is also available for those customers that want to expand their knowledge of Cisco Wireless, Cisco SDA, Cisco ISE, as well as Microsoft Server technologies beyond what is provided in this mentored implementation.

Fast Lane
www.fastlaneus.com



CUSTOM SDA MENTORED INSTALL (SDA-CUST-MI)

REVIEW HIGH-LEVEL DESIGN DOCUMENT (HLDD)

1. Review the HLDD
2. Review gap analysis if necessary
3. Review proposed policies
4. Discuss with Resource Team and make recommendations for changes if appropriate

NETWORK DEVICES UPDATE AND CONFIGURATION

1. Install new network device(s) in support of SDA
2. Update Network Device OS/Firmware if needed
3. Update network device configuration (SSH, NETCONF, SNMP, Logging, etc.)
4. Update Infrastructure ACLs if necessary

DNA CENTER (DNA-C) INSTALLATION

1. Verify DNA Center (DNA-C) appliance install and rack and stack DNA-C appliance if necessary
2. Setup and configure basic DNA-C bootstrapping
3. Verify DNA Center basic connectivity

DNA CENTER DESIGN CONFIGURATION

1. Add Sites, Building and Floor Locations
2. Add Global and/or Location Servers (DHCP server(s), DNS server(s))
3. Add Global and/or Location IP Address Pool(s)
4. Verify DNA Center Design configuration

DNA CENTER/IDENTITY SERVICES ENGINE (ISE) INTEGRATION

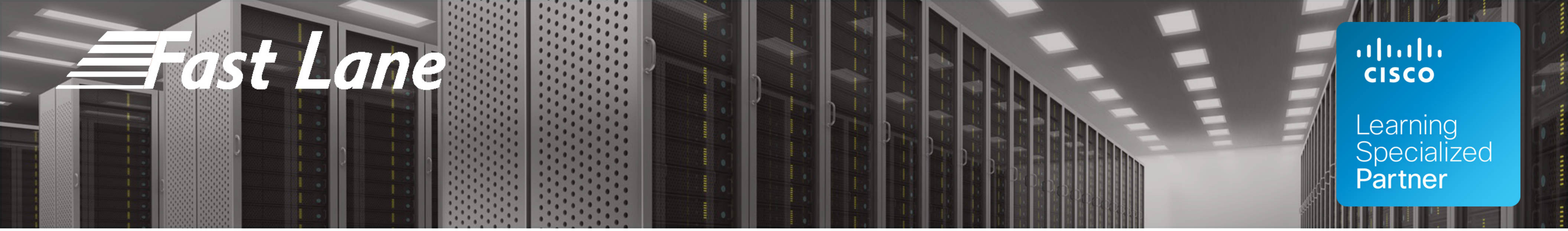
1. ISE Integration configuration in DNA Center
2. DNA Center integration configuration in ISE
    2.1. pxGrid Controller configuration
    2.2. Approve pxGrid in ISE
3. Verify DNA/ISE integration

DNA CENTER - END-HOST PROVISIONING

1. Configure SDA Fabric-Host onboarding
2. Verify end-host provisioning

DNA CENTER FABRIC PROVISION CONFIGURATION

1. Create Devices/Site mapping (what devices belong to what sites)
2. Configure SDA Fabric (select devices and mode (ex. FB, CP, FE))
3. Configure SDA Fabric - Host onboarding
4. Verify DNA Center Provision configuration



Fast Lane

cisco Learning Specialized Partner

CUSTOM SDA MENTORED INSTALL (SDA-CUST-MI)

DNA CENTER DEVICE INVENTORY

1. Add networks devices to the DNA Center device inventory
2. Verify DNA Center Inventory configuration

SDA TESTING

1. Verify SDA is working, and the traffic is flowing properly according to design

FIRST DAY SERVICE AND SUPPORT

1. Documentation hand-off
2. Remediation of customer issues

ISE POLICY PROVISIONING

1. Create/modify Policy Sets
2. Create/modify Authentication
3. Create/modify Authorization policies using Scalable Group Tags (SGT)
4. Verify ISE Provisioning

DNA CENTER INITIAL POLICY CONFIGURATION

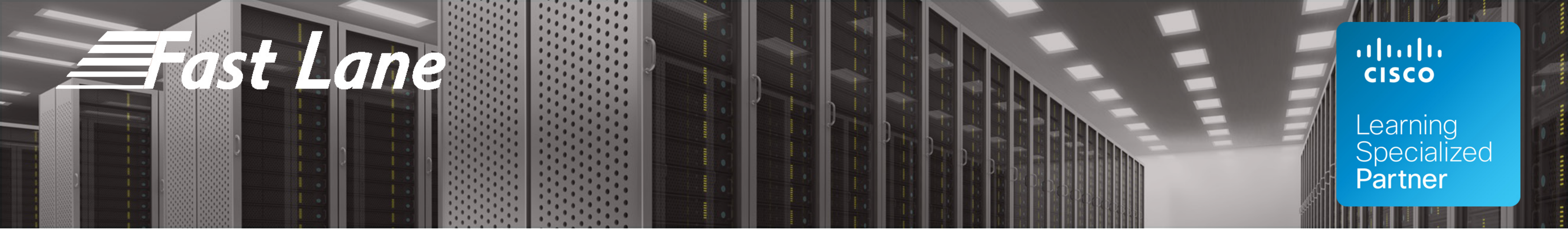
1. Verify/create Scalable Group Tags (SGT), e.g. printers, employees, contractors
2. Create Virtual Networks based on HLDD
3. Assign SGTs to Virtual Networks (VN)
4. Create custom contracts if desired
5. Create group-based access control policy
6. Verify DNA Center/ISE policy configuration

ASSURANCE REVIEW

1. Verify Assurance is collecting analytical information
2. Review analytical operations and options with customer

IDENTITY SERVICES ENGINE (ISE) NODE IMPLEMENTATION

1. Deploy ISE Appliances (virtual or physical)
   1.1. Configure Admin (PAN), Monitor (MnT), Policy Service (PSN), and pxGrid based on the HLDD
2. Install Certificates according to HLDD
3. Install Licenses as necessary
4. Configure Repository and configure backups
5. Integrate ISE Nodes with Active Directory or LDAP
6. Configure ISE Management Access polices based on HLDD
7. Create necessary users and end-user portals



PROPOSED CISCO SD-ACCESS BENEFITS

Desired Business Outcome	How We Can Make It Happen
Secure, policy-based automation	Cisco SD-Access uses policy-based automated network provisioning across all network domains as well as simple segmentation constructs to build secure boundaries for users. • Network-wide policy enforcement regardless of location • Policy administered from a central dashboard • No IP address dependency with Anycast Gateway and Scalable Group Tags (SGTs) • Single Definable policy for LAN, WLAN, and WAN
Fast, easy service enablement	Reducing the number of manual configuration steps improves network operations efficiency. The solution also quickly enables services by using open APIs across a services ecosystem. • Devices are deployed using best practice configurations • Simple user interface • Easy orchestration with objects and data models • Native third-party application hosting
Complete network visibility	The entire wired, wireless, and WAN network is managed on a single entity. Application visibility eliminates the complexity of managing separate policies for wired and wireless. • Consistent policy and management across wired and wireless • Optimal traffic flows with integrated roaming • Instantly find any user or device • Enhanced visibility helps in troubleshooting user challenges
Enhanced business analytics	The Cisco SD-Access provides intelligent services for application recognition, traffic analytics, traffic prioritization, and steering. • Detailed analytics help you plan for future growth and diversification as well as make more informed decisions • Access points (AP) tracked for performance, heat maps, and channel information • Information includes data termination of wireless traffic, network forensics, and user-based application intelligence