

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Chapter 2 Network Design Fundamentals

You are the Architect, so Your mission:

- assess the customer's current environment and its ability to satisfy their current business and technology requirements
- identify the technology shortfalls that need to be addressed
- Develop a core technology roadmap that will achieve the customer's required end-game environment
- Evaluate what is necessary for migrating successfully from one environment to another
- Create high-level architectural design and low-level detailed designs of networks devices, configurations, and interconnections

Doing the research

Who is the customer

- The business and industry the customer is in
- What sets the customer apart from competitors
- What network design will meet your customer's approval

Understanding your customer is key to a successful network design

- Business requirements and goals
- State of the current network environment
- Analyse current and future network behaviour

Engaging with the customer

Becoming a key partner

- Recognize and understand their management hierarchy
- Know who makes the decisions
- Work closely with the customer to learn their overall goals
- Understand the criteria for a successful design
- Know where the risks are and consequences for failure

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Expect some back and forth

Tool Bag? Understand what Juniper can offer the customer is key to a successful design

- Routing Devices: ACX, LN, M, MX, T, PTX
- Switching Devices: EX, QFX, OCX Series
- Security: SRX100 - SRX5800

Management solutions:

- Junos Space
- Juniper Networks Secure Analytics

Understand partner solutions:

- Load Balancing
- Secure Access
- Access Control
- Wireless

Understanding the Competition: Know who your Competition is and Confidence Key

Juniper's Lifecycle Service Approach:

- Plan (Assess, Design)
- Build (Deploy, Migrate)
- Operate (Support, Optimize)

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Plan Methodology

Assess -> Requirements -> Scope -> Data Analysis

- Requirements: identify the technology shortfalls that need to be addressed
- Scope: Determine the scope of the design project; upgrading an existing network or creating an entirely new network?
- Data Analysis: Perform a data analysis to determine the condition of the current network and what improvements need to be made
(How many users access the network internally and externally?)

Design -> Logical Design -> Physical Design

- Logical Design:
 - o High Level Design
 - o protocols used
 - o addressing
 - o security
 - o name conventions
 - o It also might include WAN and service provider access
 - Physical Design:
 - o Low Level Design
 - o Physical devices
 - o Cabling
 - o wiring considerations
 - o Service Provider access should be determined by this point
-

Chapter 3 Understanding Customer Requirements

The Request for Proposal (RFP)

Solicitation from the customer for a network design that typically includes:

- A list of design requirements
- Types of solutions the design must provide
- Warranty requirements and legal terms

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

The customer will often send the RFP to multiple vendors:

- Use responses to compare competing proposals
- Eliminate vendors who cannot meet their requirements

In some cases, you might receive a **Request for Information (RFI)**.

- typically only covers the technical aspects of the design request

RFP Key Elements

1. *Business requirements*

- Summary of what type of business the customer is in
- Vision for future growth
- Explanation of why a new design is required

2. *Environmental requirements*

- facility specifications
- number of users and workstations requirements
- Server room specifications

3. *Modular requirements*

- Hierarchical design considerations
- reduction of information within each module
- functionality of each module within the design
- In a modular design, each device has a clearly assigned function

4. *Connectivity and throughput requirements*

- Number of wireless and wired connections needed
- Traffic analysis
- Calculations for theoretical and overhead traffic

5. *Business continuity*

- Network efficiency
- Quality of service requirements
- Load balanced and highly available networks

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Always offer solutions by focusing on what your solution can do rather than what it does not support

Responding to the RFP

- Tips for a successful response:
 - o attention to the details
 - o using the format of the customer
 - o highlight benefits of your design

Response should always include:

- Executive Summary
- A network topology
- Information on the devices, protocols, technologies forming the design
- An implementation plan
- Training
- A plan for supporting and servicing the design

Defining Key Stakeholders

- Understand the Corporate Structure:
 - o Management Hierarchy
 - o Decision Makers
 - o Corporate structure
 - o Who has final say?
- Asking the right People the Right Questions:
 - o Business goals
 - o Technical goals
 - o Existing network details
 - o Technical requirements
- Understanding Corporate Politics:
 - o Hidden agendas
 - o Department relations
 - o Personnel issues
 - o Business policies

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Gathering Data

- Questionnaires
- Surveys
- Interviews
- Job Aids:
 - documentation and instructions allowing individuals to quickly access the information needed to perform a task

Traffic flow analysis

- Capacity
- Utilization
- Throughput
- Offered load
- Efficiency
- Latency

You must determine the limitations to the current network and what is required for the new network to be successful

Identifying Applications

- Identify applications the customer uses
- Include both existing and new applications
- Include user applications and system applications

Understanding Scope

Designing with modularity in mind will help you accommodate any network the customer has asked you to design

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Analyzing the Existing Environment

- working on *greenfield projects* (referred as design a network from a ground up)
 - New networks with or not restraint to consider
 - Next-generation networks created from the ground up
- adding new network to an existing architecture (*brownfield projects*)
 - Upgrading existing networks
 - old gear to be replaced
 - legacy applications that are no longer use
 - out-of-date designs that no longer make sense

Identifying resources

- Creating equipment lists
 - Bill of materials(BOM)
 - can be modular or multilevel in nature
 - More complex BOMs can be multilevel-or nested-lists whose parent devices are listed with a set of a child devices nested in two or more levels of detail.
- Setting pricing and understanding budgets
 - Create a plan that matches the customer's budget
 - Consider all expenses such as staffing, testing and training
 - does your plan eliminate jobs and add personnel?

Chapter 4 Organizing the Data

The data you have collected can be sorted into three main categories:

- customer data
- customer requirements
- project boundaries

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Data analysis

- Organizing the data can be based on: Functional area (campus, WAN, data center)
- User groups (employees, guests, remote users)
- Customer requirements

Six main categories:

1. Security
 - a. NAC
 - b. Management
 - c. Compliance
 - d. BYOD
2. Availability
 - a. Archival and Backup
 - b. Resiliency
 - c. Failover
 - d. Capacity
3. Scalability
 - a. User Base
 - b. Applications
 - c. Hardware
 - d. Performance
4. Manageability
 - a. Monitoring
 - b. Automation
 - c. Configuration Management
 - d. Auditing
5. Performance
 - a. Bandwidth
 - b. Latency
 - c. Quality of Service
 - d. Optimization
6. Budget

Identifying Design Proposal Boundaries

- Characterizing existing and future user groups, their respective applications, data flows, and data flow types
- Identifying required network parts such as campus WAN, remote office locations and the data center
- Documenting the current environment

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- Determining budgetary constraints
- Identifying the unknown boundaries that exist. This might include hidden agendas from employees, governmental laws or statutes that were not previously identified

Greenfield Versus Brownfield

Greenfield Deployments

- More options to make design module and scalable
- Very few restraints caused by existing network infrastructure

Brownfield Deployments

- More common and much more restrictive than Greenfields
- Often require integration with other vendors

User Groups and Applications

- determine the types of users that will be accessing the network and what applications they use
- enforcing security whilst maintaining accessibility
- ease of use
- performance benchmarks will be a top priority

Considering Data Flow

- you must identify the types of communication that happen-or will happen-on the network
- determining the traffic patterns currently in use-as well as calculating the data flow for future network
 - o user to user
 - o user to machine
 - o machine to machine

Functional Parts of the Network

- campus (and branch)
- WAN
- data center connections

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Exceeding Know Boundaries

- provide additional value
- make a proposal that goes beyond the know boundaries and stated customer requirements
- provide options:
 - o Good
 - o Better
 - o Best

Design Proposal Considerations

- Keep your design simple
 - Overly complex designs and customer perception
 - Considering modularity in network design
- Create the logical before the physical structure
- Consider security throughout the design process
 - Every functional area of your network topology will require some level of security within it.
- Understand the design boundaries and scope
- Remember that every choice has a trade-off
 - Security
 - Availability
 - Scalability
 - Manageability
 - Performance
 - Budget

(For example, implementing security can affect performance)
- Ensure that your proposal is clearly documented

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Capacity Planning

1. Form a discussion groups
2. Quantify user behavior
3. Quantify application behavior
4. Determine baseline existing network
5. Make Traffic projections:
 - capture data of bandwidth utilization by packet type and protocol
 - packet and frame size distribution
 - error / collision rates
6. Summarize input data for design process

Design Stages - Design Specification

- detail document of the design
 - acts as a benchmark for design changes
 - final design choices and changes need justification and documenting
 - should include change history to aid maintenance
 - used for the implementation
-

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Chapter 5 Securing the Network

- remote access, wireless devices, virtual servers, external hard drives and USB sticks are attack vector
- security threats facing networks today:
 - o Hackers
 - o Spies
 - o User authentication
 - o Viruses
 - o Worms
 - o Trojans
 - o Wired Users
 - o BYOD
 - o Guest users
 - o SQL Injection
 - o password cracking
 - o DDoS

Common security requirements:

- User authentication
- Access control
- Firewall and zone-based segmentation
- IDP
- UTM
- Point-of-sale (PoS) compliance (typically branch only)

Does the customer have a compliance reason for security?

- PCI-compliance, SOX, and so on
- How much access do the users need?
- Will full Internet access be required?
- Will users need to authenticate for network access?
- How much security can the enterprise manage?

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Context Awareness

- Which user?
- What application?
- Which device?
- Which location?

Authentication

- Wired and wireless authentication
- 802.1x, EAP but other methods might be used
- Enables role-based access control:
 - Allows access to resources or networks based on user-credentials such as group membership
 - Enables detailed logging and accounting of user activity
- Authenticate every device every time
 - Enables the highest levels of network security
 - Must support smartphone and tablet users
- *Network Access Control (NAC)*
 - become essential for enterprise networks
 - increasing number of remote workers, contract workers and other guests on the network

Defining Security Policies

- policies are needed to communicate between zones
- policy Components:
 - o Zones
 - o Source
 - o Destination
 - o application and match criteria
- authentication: will policy require firewall, UAC or VPN authentication
- Do not forget about deny rules and placement !!!
- Security Policy Best Practices
 - o Summarize IP addressing wherever possible
 - o Use address-sets and service-groups
 - o add a deny all rule with session logging last

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Intrusion Detection and Prevention (IDP) best practices

- security Policies:
 - o on which policies should we enable IDP
 - o detect-only or drop traffic
 - o might want to start out in detect-only mode
 - o analyze real-world traffic for false-positives
 - o User custom signature groups that exclude false-positives
 - o Change configuration to begin dropping attacks
- recommended signatures
- custom signature groups

Unified Threat Management (UTM) best practices

- Antivirus
 - URL filtering
 - Antispam
 - Intrusion Prevention
- Where will UTM be enforced?
- From branch users and guests to internet?
 - From internet to branch guest users?
 - From branch users to centralized services?
 - Inbound traffic from data center to branch?
 - Traffic between branches?
- Security Policies: which ones should we enable UTM?
- Antivirus UTM policies: Outbound (to Internet) matching HTTP and FTP
 - URL filtering UTM policies: Typically enabled on outbound (to Internet) Web traffic only

PCI Compliance

- Devices processing transactions must be isolated from other network nodes
- Account information cannot be stored or transmitted in unsecure fashions
- Firewall policy, reporting and centralized management are key criteria
- Authenticate network access

Being able to demonstrate PCI compliance to the auditors is important for a yearly report on compliance (ROC)

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

WAN Security

Identify the untrusted domains and determine plan to monitor, manage and mitigate all security risks

- Public Model:

- Service Provider provides transparent MPLS service to the customer
- No management required by the customer
- Security through MPLS

- Hybrid Model

- Customer manages CPE devices: traffic is again secured through MPLS
- Home users and remote sites are secured using IPsec tunnels

Data Center Security Requirements

- Scalable performance
- Interface flexibility: Scale the Firewall without re-architecting the network
- System and network resiliency: Carrier-class reliability; separation of data and control planes
- Network segmentation capabilities
- Flexible network integration

Data Center Security Challenges:

- Performance requirements
 - o Traffic throughout
 - o connection per second
 - o sustained total connections
 - o latency
- Resiliency requirements
- Scalability
- Network Integration: Routing and Virtualization capabilities

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Security Design Considerations:

- Consolidation and virtualization
- Security versus performance tradeoffs
- On-demand resource allocation
- Polymorphic nature of new applications
- Evolving threat landscape
- Control over all the traffic client to server, server to server, and server to client
- High performance and security at scale
- Application Layer visibility and control
- Identity-aware dynamic security protection
- Consistent security posture in on-demand resource allocation environments
- Unified management and monitoring

Incorporating Data Center Security

- Security should be incorporated at the perimeter of the data center for north and south traffic flows and between the servers for west and east traffic flows
- Junos Space:
 - o next-generation application platform designed to managed next-generation networks
 - o simplifies network operations
 - o scales services
 - o automates support
 - o installable applications within Junos Space:
 - Network Director
 - Edges Services Director
 - Security Director: deploy end-to-end security services on network elements (Firewall policy, IPS, NAT, VPN)
 - Content Director
 - Virtual Director: deploy, manage, and monitor vSRX instances
 - Services Activation Director
 - Service Insight
 - Service Now

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Chapter 6 Creating the Design-Campus

Campus Topologies (see Appendix)

- Horizontal
- Vertical
- Metro Campus
- Widely distributed
- Hub and Satellite

Legacy 3-Tier Design

- Complex
- Inefficient
- Costly
- Oversubscribed

Consolidating Security:

- Eliminates multiple devices
- Improves efficiency
- Lower latency
- Lower power, cooling and space costs

Collapsing Layers:

- Simplifies operations
- Reduces the number of devices
- Reduced number of uplinks
- Reduced latency

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Design Guidelines for the Campus

- Ensure design is secure and protects customer resources
- Ensure design allows for network resource availability
- Ensure design is easy to deploy and operate
 - Minimal configuration required
 - Easily supports deployment of advanced services such as video, UC and virtualization
 - Limits the number of platforms to learn, maintain, and spare
 - Eliminates blocked links caused by STP and FHRP
- Knowing the Trends and Requirements
- User driven wireless networking requirements:
 - 1 AP per 10-15 users or per 400 square feet of coverage area
 - Reserve 10% of wired ports for wireless APs
- Subnet Design
- Device Naming Conventions
- Using the Top-Down Design Approach:
 - Knowing users, applications, traffic types and traffic patterns can help determine the best network design
- *Over Subscription ratios:*
 - Over subscription ratios identify the ingress to egress link bandwidth in a south to north direction in the network
 - Switches are generally categorized as having a non-blocking architecture or a blocking architectures
 - a non-blocking architecture means that the switch's internal resources can accommodate ingress and egress
 - traffic flows at their maximum rate
 - some architects use a 20:1 ratio for the access-distribution uplink as a general starting Point

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- Campus Core:

- Legacy Campus Architecture
- Oversubscribed interfaces require additional links
- Each wiring closet and each aggregation core device must be managed
- Can be complex to manage and troubleshoot

Security Through Isolation

- BYOD Through Isolation:
Place guest users and devices in an isolated VLAN, such as a guest VLAN, and ideally a unique routing instance
- VLAN Connectivity:
 - Create a standard VLAN schema used on all access switches
- Access Control Design
 - 802.1x EAP provides access control
 - 802.1x can be used to authenticate user ports
 - MAC authentication can be used to authenticate other devices
(that do not support 802.1x)
 - *single mode* authenticates only the first supplicant
 - allows only one supplicant to connect to the port
 - multiple mode allows multiples supplicants
 - each supplicant is authenticated individually

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Common Configuration Scenarios

1. Layer 2 Access Looped Topology
 - Physical Topology - No Virtual Chassis
 - Logical Topology - Virtual Chassis at Aggregation
 - Logical Topology - Virtual Chassis at Aggregation and Access
 2. Layer 2 Access Loop-Free Topology
 - Physical Topology - No Virtual Chassis
 - Logical Topology - Virtual Chassis at Aggregation
 - Logical Topology - Virtual Chassis at Aggregation and Access
 3. Layer 3 Access Loop-free Topology
 - Physical Topology - No Virtual Chassis
 - o all paths forwarding (OSPF ECMP)
 - o fast convergence
 - o L3 license costs
 - Logical Topology - Virtual Chassis at Aggregation
 - o all links forwarding (LAG)
 - Logical Topology - Virtual Chassis at Aggregation and Access
 - o Fewer unique access switch configurations
 - spanning-tree protocols still required if access layer must interface with traditional tiered environment (migration or brownfield expansion scenarios)
 - Root Bridge Placement
 - Spanning Tree Protection features:
 - o root protection
 - o bpdu protection
 - o loop protection
-

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Chapter 7 Creating the Design-WAN

Wide Area Network Defined

- A wide area network (WAN) is a network covering a broad and geographically dispersed area that is used to interconnect business locations and resources.
- Enterprise WAN connectivity functions:
 - *Internet Edge*: The internet edge function is typically found in the campus, branch and data center environments
 - *WAN (Branch) Aggregation*: The WAN aggregation function connects remote branch offices to the main campus network
 - *Private WAN*: The private WAN function connects all enterprise sites and servers as the corporate-managed backbone
 - *Data Center Interconnect*: the data center interconnect function connects all corporate data center locations
 - disaster recovery / business continuity
 - data center consolidation and virtualization
 - Geo-clustering
 - Layer 2 extensions for any reason

Enterprise WAN Design Goals

- Easy to deploy
- Flexible and Scalable
- Resilient and Secure
- Easy to Manage
- Service Ready

Connectivity Considerations

- What WAN connectivity options are available?
- Where will a backup WAN connection be required?
- What type of WAN connectivity will be used?
 - Private WAN (multiple classes of service)
 - Public Internet
 - Provider-Managed MPLS Service (4 classes of service typically available)

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

WAN Device Roles

- WAN aggregation
- Internet Gateway
- VPN Termination

Determining Throughput Requirements

- the number of users and devices
- applications and their associated traffic flows

Performing Considerations

- the speed and latency of the WAN are often the main bottleneck between sites in an enterprise network
- the smaller packets such as voice and video will impact performance the most; therefore when evaluating a router's performance
 - o we recommend using internet mix (IMIX) which is a mix of packet size
- Consider the following when designing a flexible branch network:
 - Extra capacity can be added on the same platform or by adding additional devices without disrupting the network
 - flexibility to add feature support in the future such as different dynamic path discovery protocols
 - service flexibility to facilitate the introduction of services such as firewall or IPS on same platform
 - different network virtualization techniques
 - advanced QoS functionalities
- Flexibility can come with higher capital expenditures (CapEx) initially. However, it provides both lower CapEx and operational expenditures (OpEx) in the long term.

VPN Design Considerations

- Tunneling packets in IPsec increases packet size
- Additional overhead can exceed 36 bytes
- Must limit the size of packets pre-encryption

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- Enforced by limiting the MTU size of IPsec traffic
 - TCP-MSS size when using IPsec:
 - IPsec tunnel mode with no NAT transversal: 1463 bytes
 - IPsec tunnel mode with NAT transversal (UDP): 1400 bytes

Using Virtual Routers

- Enterprise WAN have the ability to configure multiple routing instances, which are also know as virtual routers (VRs)
- Additional scenarios where traffic might have to be kept separate using routing instances include:
 - o Merging organizations
 - o Multi-tenant buildings
 - o Secure facilities
 - o College campuses

Enterprise WAN: Active / Passive Design

Enterprise WAN: Active / Active Design

- A WAN router at the remote branch location has two independent WAN connections to two distinct Layer 3 VPN service Providers
- each WAN connection is active

Enterprise WAN VPN Design Options

- 2-Tier Design - Branch to VPN Termination Device
 - 3-Tier Design - Branch to VPN Termination Device and Branch to Data Center
 - Full Mesh Design - Branch to Branch, Branch to VPN Termination and Branch to Data Center
-

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Chapter 8 Creating the Design-Data Center

What is a Data Center?

A closet, room, floor or entire facility that houses the computing resources and services used by a company

Components:

- WAN Domain
- Security Domain
- Layer 2 and Layer 3 Infrastructure Domain
- Compute and Storage Domain
- Management Domain

Traditional Data Centers

- most data center access switches are deployed at *top-of-rack (TOR)*, *bottom-of-rack (BOR)*, *middle-of-row (MOR)* or at *end-of-row (EOR)*
- the switches required in the aggregation and core tiers are typically line-rate, nonblocking switches
- using a traditional hierarchical network design in the data center has a number of challenges:
 - Limited scalability
 - Inefficient resource usage
 - Increased latency

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Assessing the Data Center Needs

Some key questions to ask the customer include:

- Does the data center deliver revenue generating services or does it support your internal IT and campus environments?
- In addition your main data center network, how many other data centers do you have? Will they interconnect?
- What are the grow plans for the server farm for the next two years? Are they 1GBe or 10GBe server ports?
- What are your performance requirements?
- Do you need traffic separation or SLAs?

Categorizing Data Centers

- Data centers vary significantly in size, performance, function and requirements:
 - Enterprise IT-CapEx and OpEx, server virtualization
 - Public Clouds - Massive scale, Scale out
 - Performance Oriented – Low latency, Low jitter, High performance

Design Guidelines and Requirements

- Common guidelines and requirements:
 - Lower total cost of operations and investment protection
 - data center consolidation
 - energy and space
 - A simple, high performing and highly available environment
 - increased bandwidth and lower latency
 - high availability, reliability and modular scalability
 - simpler, flatter network
 - storage awareness, network convergence and virtualization
 - Aware of users and applications
 - Integration of user, application, network and security policies
 - Layer 2 mobility throughout data center

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Understand the Trends

- Data Centers are moving to a service-centric structure:
 - Storage Pool
 - Shared Services
 - Compute Pool
- Data Centers are moving to a collapsed structure
 - Why do Traffic Patterns Matter?
 - Determining the flow and patterns of traffic and the data center helps you identify capacity requirements!
- Building the Foundation:
 - The size and characteristics of the access tier create the foundation of the entire data center network
 - The size of the aggregation and core tiers and the number of uplinks is largely determined by the size of the access tier

Using Virtual Chassis in the Design

- Inserting Virtual Chassis in to the design can:
 - Simplify the design and management operations
 - Improve scale, performance and high availability
 - Reduce cost (cabling, uplinks and equipment)
- Virtual Chassis allow up to 10 switches, interconnected through using interchassis connections, which may use either special backplane cables or using 1GbE or 10GbE uplinks. The result is up to 10 line cards that fitting into a single chassis
- Depending on the design, a Spanning tree may not always be required because the member switches functions as a single switch
- This logical switch is maintained through a single active configuration file.
 - Juniper recommends that all switches in a Virtual Chassis configuration be connected in a ring topology.

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Layer 2 at the Access Tier design considerations:

- Architecture and protocol deployment options include Virtual Chassis, xSTP, LAG and RTG
- Challenges include spanning-tree scaling, fault containment, loop prevention and blocked spanning-tree links

Layer 3 at the Access Tier design considerations:

- Architecture and protocol deployment options include Virtual Chassis, LGA, IGP and BFD
- Layer 2 domain and Layer 2 mobility are both restricted to a set of access elements

Simplifying the Topology Further - using Virtual Chassis technology in the aggregation tier:

- Eliminates or minimizes control plane complexity (such as STP or VRRP)
- Utilizes all uplinks with standards-based, cross-chassis LAG (increases effective uplink bandwidth)

Incorporating Security

Security should be incorporated at the perimeter of the data center for north and south traffic flows and between the servers for west and east traffic flows

Data Center Architectures

- Traditional Layer 2
- Tier-MC-LAG
- Virtual Chassis
- Virtual Chassis Fabric
- QFabric
- Layer 3 Clos

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Selecting a Design Profile Template

- profiles:

- Transactional
- Mid-Tier
- Enterprise IT
- HPC
- Content Services Hosting

- the three *key dimensions* of a data center *profile*:

- Functionality (routing, security and availability)
 - Cost (capex, opex and TCO)
 - Performance (latency, throughput and oversubscription)
-

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Chapter 9 Business Continuity and Network Enhancements

Business Continuity is:

- An organization's need to ensure that essential functions can continue during and after a disaster
- The prevention of interruption to mission-critical services
- The ability to re-establish full functionality as quickly as possible following a disaster
- Disaster recovery is not business continuity

Business Continuity Planning

1. Know your network

- List all functions and services
- Perform a Business Impact Analysis to determine:
 - Which functions and services are critical to the company survival
 - The cost of both partial and full outages-downtime equals money lost
 - How long could an outage be sustained?

2. Risk Assessment

- What hazards might affect your business?
 - IT failure / loss of data
 - Flooding
 - Power loss
 - Fire
- Considered in terms of:
 - Impact
 - Likelihood

3. Formulate the Plan

- You cannot plan for everything
- Use the risk assessment to plan for the most likely ones

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

4. Test the Plan

- Staff must be notified and know what is expected of them in response and recovery
- After the testing
 - Review
 - Revise
 - Retest

Resiliency

- What are the *uptime requirements*?
- While the customer will typically say "no downtime", in reality there will always be some downtime
- Customers plan for known and unknown downtime and target availability
- 99.9% availability tells them downtime cannot exceed 10 minutes per week average
 - Three Nines 99.9% availability means only 10 minutes of total downtime per week (planned and unplanned)
- What can affect the uptime of the network?
 - Power outage
 - WAN failure
 - Device power supply failure
 - Device failure
 - Device firmware upgrades or reboots
 - Planned outages (for upgrades or migrations)

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Building a Highly Resilient Network

- Link-level redundancy (multiple WAN connections and physical uplinks)
 - When does a second or backup WAN link make sense?
 - When your service provider cannot meet your SLA
 - when your enterprise relies on VoIP or Unified Communications
 - any time the cost of a second link is less then the cost of downtime
- Device-level redundancy (redundant hot-swappable interfaces and power supplies)
 - When does a redundant power supply or processing blade make sense?
 - Any time redundant power from two sources is provided at the customer premises
 - Connect each power supply to a separate power source
 - When a two-device HA solution is not used due to costs or complexity
 - A second power supply provides some guarantee against device failure
- Physical device redundancy (redundant devices, VC)
 - When does a physical device redundancy make sense?
 - When a HA profile is desired (+3 nines or < 10 minutes per week)
 - Any time downtime cannot be afforded due to firmware upgrades or devices reboots
 - When zero impact to users and applications is required during failures

Virtual Router Redundancy Protocol (VRRP)

- supported on EX Series and MX routers
- standard RFC 2338

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Chassis Clustering

- Connects **two** identical SRX Series devices into a single logical device
- Uses a *control link* and a *fabric link* to connect the two devices
- Types:
 - Basic Active / Standby
 - The goal of a cluster is to be able to move or failover traffic flow from one box to other when needed.
 - To help accomplish this, a special interface type is used: *redundant ethernet (reth)*
 - ~ A reth interface is a virtual interface
 - ~ it is active on one of the two nodes only and it has the ability to move or failover to the other node
 - ~ when a reth interface fails over to the other node, all its logical interfaces also failover and become active on the other node
 - Chassis Cluster Active / Standby with multiple reth interfaces
 - Chassis Cluster Active / Standby with LAG
- the Small Branch:
 - SRX device handles routing and security while EX device does switching
 - Supports multiple WAN connections and WAN failover
- the High Availability Small Branch:
 - SRX device HA cluster handles routing and security, while EX device cluster handles switching
 - Supports multiple WAN connections and WAN failover
- the HA Large Branch:
 - 2-tier design uses routing between SRX devices and EX switches for HA
 - SRX device HA cluster handles routing and security, while EX device cluster handles switching
 - Supports multiple WAN connections and WAN failover

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Multi-chassis link aggregation

- allows you avoid the single point of failure scenario when a switch fails
- LAG is split between two upstream switches appearing as a single switch to downstream device
- MC-LAG positioning scenarios:
 - In data centers, MC-LAGs are commonly positioned between servers and the access switches (TORs) as well as between the distribution and core switches

Campus Redundancy Best Practises

- Highly available redundant LAN and wireless access for all applications
- Network redundancy, multiple uplinks and network paths distributed across multiple devices
- Hardware redundancy:
 - Redundancy Routing Engines
 - network fabric, power and fans
- Redundant wireless access points are clustered and distributed to provide seamless roaming
 - Density of access point should provide wire-like reliability and performance

Virtual Chassis

- VC provides 2+N control plane redundancy, where the two Routing Engines have the role of master and backup
- has a dual-ring control ring control plane, which can be created either using a 128 Gbps VC fabric connection or over a link aggregation connection using a standard network port
- design considerations:
 - can include between two and ten switches
 - Port density factor
 - Resilient factor: the more switches, the higher the availability
 - System cost: the more switches, the higher the cost

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- positioning:

- WAN

- MX Series two member Virtual Chassis in the core
- *graceful Routing Engine switchover (GRES)* and *Nonstop active routing (NSR)* must be enabled on both
- you can configure a VC on the following MX Series with *Trio Modular Port Concentrator (MPC)*, *Modular Interface Controller (MIC)* interfaces (for configuration of VC ports) and dual Routing Engines:

- MX 240

- MX 480

- MX 960

- Data Center

- convenient placement leads to significant savings in cabling cost
- TOR, BOR, across racks and across rows

Virtual Chassis Fabric

- Two or more interconnected QFX Series, EX Series or both switch types operating as a single VCF system
- up to 20 switches can be member
- Leaf or Spine
- QFX5100 can be placed in the Spine or Leaf location
- QFX3500, QFX3600 and EX4300 should only be wired as Leaf devices in a mixed scenario

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Similarities Between VCF and VC

- Member ID = FPC slot
- Console and management sessions (SSH, Telnet) are redirect to the master RE
- Uses *Virtual Chassis Control Protocol (VCCP)* to discover the fabric topology
- Supports pre-provisioned and non-provisioned (dynamic) VCF enablement
- When two or more local interconnects exist between two nodes, the interconnects are automatically placed into a LAG for load-balancing and redundancy

Differences Between VCF and VC

- VCF can support up to 20 members switches
 - It is the logical upgrade when a Virtual Chassis has reached its capacity
- VCF uses a Spine and Leaf architecture instead of typical ring topology of a Virtual Chassis
 - Based on a Clos three stage (folded) switching fabric
- When multiple paths exist between members, traffic is load balanced across the paths
 - In Virtual Chassis, only a single path is ever used (assumes VCP LAG bundle represents a single path)
- supports Automatic Provisioning

VCF Best Practises

- Spine nodes must be QFX5100 Series switches
- RE role must only be assigned to Spine nodes
- all leafs should be configured for line card role
- every Leaf node should connect by VCP to every Spine node
- use either all 40Gbps VCPs or all 10Gbps VCPs
- QFX5100 should be used as Spine node
- use either 2 or 4 Spine nodes (better load balancing)
- all Spine nodes should be configured for RE role

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Quality of Service and Class of Service

- The goal of QoS technology is to deliver predictable application performance throughout the network
- Best effort delivery is not acceptable for time sensitive traffic such as voice and video
- QoS is experienced end-to-end
 - A single hop without QoS can ruin the end-to-end QoS experience
- CoS is the treatment of traffic at an individual node
 - ultimate goal is to ensure consistent end-to-end QoS
- understanding Packet Flow Across a Network:
 - CoS examines traffic entering the edge of the network
 - Traffic is classified into different groups, each receiving different treatment
 - Traffic is reclassified as it leaves the network at the edge
 - CoS must be configured on each router in the network
- Network Traffic Congestion:
 - Attributed to the hardware itself or to the network deployment
 - If a device does not have congestion management features, packets will be dropped or latency will be introduced
 - In a TCP/P network, dropped packets will be retransmitted, further increasing the network load
 - Traffic congestion management is especially important for time sensitive data and applications such as voice and video
- CoS is recommended as a possible solution when users are experiencing the following:
 - Timeouts or long delays from applications
 - Voice or video quality issues
 - Choppy or clipped voice transmissions
 - Pixilation or constant buffering of video streams

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

CoS in the Campus Network

- Convergence of voice and data networks
- Differentiation between applications or types of users
- Guaranteed bandwidth, especially on low-speed links

Junos CoS

- The Junos OS provides a full-featured set of CoS mechanisms:
 - 32 forwarding classes
 - 8 queues
 - Supports a common set of features from the access layer to the core
- Careful planning is required to ensure the CoS configuration is consistent across all devices
- Equipment across the CoS domain must be interoperable

Data Center Physical Layout

- Multiple physical divisions:
 - Referred to as segments, zones, cells or pods
- physical Considerations:
 - Placement of equipment
 - Cabling requirements and restrictions
 - Power and cooling requirements
- Layout options:
 - *Top of rack (ToR)*
 - *Bottom of rack (BoR)*
 - *Middle of row (MoR)*
 - *End of row (EoR)*
- data center cabling:
 - Cabling is a major cost in the data center
 - Any major change to the data center will involve the need to run new cable

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- Planning for 40-Gigabit Ethernet and 100-Gigabit Ethernet:
 - Higher bandwidth will be needed in the data center
 - The IEEE has defined standard for 40-Gigabit and 100-Gigabit Ethernet
 - Future-Proofing Data Center Cabling:
 - Specify minimum of OM3 fiber
 - OM4 as an option for extra reach
 - Design data centers for 100-150 meter maximum lengths between switches
 - Consider higher fiber count requirements
 - 2 fibers per link becomes 24 fibers
 - MTP (or MPO) connectors will become the standard transceiver interface, compared to LC connectors
 - Consider cable management and structured cabling
- Hot and Cold Aisle Design
 - Cool air is drawn in from a common cold aisle
 - Hot air is exhausted out a common hot aisle
 - Having as much separation and containment of hot and cold air as possible is desirable
 - Helps avoid hot spots within the data center
 - Enabling Hot Aisle/Cold Aisle Design:
 - Many Rack are designed to assist air flow cold aisle to hot aisle
 - Raised floors with perforated tiles, ducts and plenums can also be used to control air flow
- power considerations:
 - Electricity costs rose 88% in the US since 2003

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- physical Plant Limitations and Efficiencies:

- Equipment selections now include space, power and cooling efficiency metrics
- Equipment placement within data centers is often directly related to cooling patterns and power grid design
- Achieving these physical goals in conjunction with logical service delivery requirements is critical
- Real estate budgets limit data center size (in ft² or m²)
 - Goal is to obtain maximum results from a defined footprint
 - Use metrics such as ports per rack, servers per rack, workloads per data center
- Power costs are a major factor in a viable design
 - Requires maximum efficiency in design and utilization
 - Some new data centers are located close to cheaper, greener power
- Up to 50% of power costs are for cooling
 - Design equipment and data center layouts for maximum cooling efficiency

- Energy Efficiency in Equipment Design

- Sufficient and affordable power is an important determination of design
 - Servers and storage require more energy, in total, than network
 - Network industry has formed the ECR Initiative to form a common baseline for measuring energy use in equipment
 - energy efficiency ratio (EER = Gbps/KW) is the widely used comparison metric
 - Allows comparison of similar configurations on energy use
-

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Chapter 10 Network Management and Automation

Network Management

- Network management is a broad topic and means different things to different people
- Reasons for network management:
 - Manageability
 - Measurement
 - Planning (for the future)
 - Decreasing downtime
 - Configuration
 - Accounting

Network Management Methodologies

FCAPS Model

- F - Fault management
- C - Configuration management
- A - Accounting management
- P - Performance management
- S - Security management

OAMP(T) Model

- O - Operations
- A - Administration
- M - Maintenance
- P - Provisioning
- (T) - Troubleshooting

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Separate Network Management and Production Networks

- Production network loads or failures should not impact the ability to monitor and control the network infrastructure
 - Access to device and network performance and fault information is most crucial when the network is in a failure mode
- Separation at the physical interface-level is preferable to logical separation
- Separating production and management networks:
 - Mitigates bandwidth contention (performance)
 - Simplifies data collection and analysis (management traffic volumes do not skew reported production traffic volumes)

Configuration Management

- Consistent approach for physical layout expedites deployment as well as diagnostics:
 - Standardize rack layout
 - Standardize device slot and module population
- Keep like devices running identical software and firmware:
 - Expedites troubleshooting
 - Simplifies sparing and replacing
 - Determination of software versus hardware is much more obvious
- Configuration Management Technics:
 - Define a device naming convention and follow it
 - Consistency in naming:
 - Eases automation of DNS zone edits
 - Simplifies pattern matching logic
 - Expedites physically locating devices
 - Brevity is good, so resist encoding too many things into a hostname (consider using DNS subdomains)
 - Make use of description fields in device configurations:
 - Just like hostnames, define a convention and follow it strictly

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- Backup
- Provide Secure remote Console Access:
 - Device failure is imminent
 - Failure modes are seldom convenient:
 - Many failure modes of network equipment render remote in-band access impossible, leaving only the console port
 - Ready access to all device serial consoles is critical:
 - Even if resources are onsite 24/7 you do not want to rely on being able to find the right combination of cables, adapters, and terminal emulation tools when you need them
 - Permanently connect serial consoles to dedicated console server ports
 - Ensure that console servers can provide remote IP terminal connectivity to the device serial ports - but only from trusted IP networks
 - Configure (and clearly label) one or more serial ports on the console server to provide locally-connected terminal access to the other ports:
 - Allows device console access even if the management IP network fails
 - Ensure that proper serial cables and adapters are always available for local console server access

Baseline Network Behaviours

- A reference is necessary for good performance or normal behaviour in your network
- Continuous monitoring and data collection creates a historical baseline of your network's normal behaviour
- Failures and anomalies become easier to detect once these normal behaviours are established
- Baseline network behaviors takes place in multiple planes:
 - Gross load and error rates
 - Traffic type and direction
 - Application-level behaviors

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- Tools are available to baseline:
 - SNMP data collectors
 - Flow Collection and reporting tools
 - Topology-aware tools
 - DPI tools
- The more detailed knowledge you have about your network's traffic and flows, the easier managing for optimum performance and reliability becomes
- Leverage Authentication, Authorization and Accounting Systems
 - Centralizes control of authentication-Enable finer-grain accountability
 - AAA servers can enable features not available for device-local authentication
 - Password expiration
 - Two-factor authentication
 - Use of least privileged approach for profiles minimizes exposure
 - The value of centralized AAA increases exponentially with the number of devices

Delegate Data Collection and Reduction

- Data collection and thresholding using RMON alarms
 - Data collected and analysed on-device
 - NMS notification on threshold crossings
- Considerations needed for proper threshold baselining and device resources
 - RPM
 - Distribute response time monitoring into network devices
 - Detect and report data-plane performance degradation that would be transparent to other instrumentation
 - Notification reduction using event policy
 - Event data reduction on-device by defining event policies
- Keep Things as Simple as Possible
- always favour obvious over clever in automation scripts or network configurations

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Junos Space

(described before)

Network Director

- Unified wired and wireless network management solution
- modes:
 - Build
 - Deploy
 - Monitor
 - Fault
 - Report

Security Director

- Deploy end-to-end security services on network elements:
 - Firewall
 - VPNs
 - NAT
 - UTM
 - Application Services
 - IPS
- Junos Space centrally manages the security policy lifecycle
- Event Collection Challenges:
 - IT information overload
 - Compliance mandates
 - Evolving internal and external threats

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Juniper Secure Analytics

- Network Security management
 - Collection of security event and network traffic monitoring
 - Normalizations and mapping of all data to a single format for processing and storage
- Network security management requirements:
 - Data analysis and correlation
 - Notifications and alarms
 - Operation and compliance reporting
- JSA Device Key Benefits
 - Converged network security management console
 - Network, security, application and identity awareness
 - Advanced analytics and threat detection
 - Compliance-driven capabilities
 - Scalable distributed log collection and archival

Automate Device Configuration

- Automation is crucial for scalability
- Configuration automation provides consistency
- NMS-based device configuration
 - Junos Space (Network Director)
 - Rancid
 - Solarwinds, Puppet, Chef, Ansible, Open NMS
- For Junos devices, this automation can be achieved from within the devices themselves
- Commit scripts:
 - Run at commit time
 - Inspect the incoming configuration
 - Instruct the management daemon to perform actions

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- Commit script allow customers better control over how their devices are configured
 - Programmatically constrain device configurations according to network architecture constraints
 - Defend against common errors by correcting device configurations automatically
- Enabled customized configuration syntax to streamline configuration
- Commit scripts can constrain device configuration
 - Codify customer-specific business rules
 - Block configurations that break the rules
 - examples:
 - Insist that each ATM interface does not have more than 1000 PVCs configured
 - Insist that an IGP does not use an import policy that will import full routing table
 - Insist that all LDP-enabled interfaces are configured for an IGP
 - Insist that the re0 and re1 configuration groups are set up correctly and that nothing in the foreground configuration is blocking their proper inheritance
 - result:
 - Configuration problems are detected and prevented
- Device configurations can be auto-corrected
- Commit scripts can change configuration:
 - Correct errors as they are detected
 - Flesh out configuration based on implicit rules
 - Examples:
 - Automatically build a protocols ospf group containing every Ethernet interface configured under [interfaces]
 - Automatically configure family iso on any interface with family mpls
 - Apply a configuration group for any SONET interface with a description string matching a particular regular expression
 - result:
 - Problems are prevented before they occur

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Automate repetitive Diagnostic Functions

- Typically, fault diagnosis is performed by following a set of written procedure from a network operations center handbook or something similar
- Most procedure can be automated
- Automating these repetitive diagnostic tasks:
 - Enforces consistency
 - Allow operators and engineers to focus on problem analysis, not data collection

On-device Diagnostic Automation

- On-Device diagnostic scripts are op scripts and event scripts
 - Perform any function through RPC supported by Junos NETCONF / XML API and Junos Automation
- *Automation scripts* allow:
 - Automatic diagnosis and repair of network problems
 - Changing device configuration in response to a problem
- *Op scripts*:
 - Execute any Junos command
 - Results can be captured, processed and automatically delivered to the CLI or remote systems
- *Event scripts*:
 - Can execute Junos commands or scripts, in response to an event policy
 - Occurrence of specific syslog messages or traps
 - Very similar to op scripts but can also operate on data received from the Junos event subsystem

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

Network Management Platform Based Diagnostic Automation

- Can leverage access to device-based diagnostics:
 - Request execution of an op script on a router or switch
 - Request execution of ad-hoc native commands on devices
- Can compare diagnostic output from multiple devices at the same time
- Can leverage access to other management data:
 - Historical performance data-plane
 - Trouble-ticket history
 - Customer contact data
 - Circuit database

Chef for Junos

- Software that automates provisioning and management of compute, network and storage solutions (VMs)
 - Abstract definitions written in Ruby and applied to infrastructure nodes running Chef clients

Junos PyEZ

- Python-based micro-framework to remotely manage to automate Junos OS devices
- Built for non-programmers and programmers alike
- Built on top of community provided nc-client library

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

SDN

- A different approach to designing, building, and managing networks
 - Provision for flexible and dynamic networks
 - Change how software works in a network
- A solution to the current challenges of the network
 - Networks must adjust and respond dynamically
 - Newly added feature must not disrupt the network
 - Alleviate the need for manual configuration of individual devices
- Separates the control plane from the forwarding plane
- SDN knows the entire network - all paths
 - Control plane moved to the SDN controller
 - Forwarding plane remains on switches
 - Optimal path selected
 - Redundant paths available

Contrail

- SDN Solution
 - Automates and Orchestrates virtual networks
 - *Network Functions Virtualization (NFV)*
 - Big Data
 - Visualization
- Two primary drivers
 - Cloud networking
 - NFV in service provider network
- Building Blocks:
 - Basic Abstractions
- Virtual Machines
 - Cloud tenants
 - Virtual Network Functions

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- Virtual Networks

- Connect VMs

- Gateway Devices

Contrail Solution

- Orchestrator (OpenStack, CloudStack)

Chapter 11 Putting Network Design into Practice

Network Design Checklist

1. Process for understanding the customer's business and technical goals
2. Validation process for analysing customer's existing environment
3. Steps for designing a network topology
4. Process for selecting protocols, address schemes, naming conventions and so forth
5. Steps for implementing a security strategy
6. Process for developing a network management and automation solution
7. steps for testing, optimizing, and implementing your design

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

RFP response

- An execute summary
 - Executive Summary Key facts:
 - The single most important part of the proposal
 - Overview of Juniper's value proposition to the customer
 - The only part of the document that will likely be read by all decision makers
 - Understanding Customer Needs
 - Address the customer's key requirements
 - Use the customer's terminology and formatting
 - Outline the benefits of choosing your design
 - Golden Rules
 1. Make it understandable to the customer
 2. Focus on organizational issues
 3. Keep it short and simple
 4. Avoid canned responses
 5. Avoid cliches
 6. Avoid history lessons
 - Recommended *structure*
 1. Introduction of the customer's need or problem
 2. Identification of business benefits
 3. Overview of your proposal solution
 4. Relevant supporting information outlining why the customer should choose your plan and Juniper Networks
 - Closing Statement:
 - Ask for the business
 - Treat the customer as an equal

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

- A solution overview
 - Technical summary of your proposed solution
 - Address customer goals, scope and requirements
 - Outline technical benefits
 - Keep it short and simple
 - Assume that executives will read this section
 - Technical specifications
 - responding to Technical Specifications
 - Outline the technical details of your proposal
 - Respond to the customer's RFP requirements
 - Include design requirements
 - logical and physical topologies
 - Bill of materials
 - Implementation roadmaps
-

Chapter 12 Network Migration Strategies

Juniper Networks' Migration Methodology

- Current State -> Analysis -> Migration Plan -> Migration Execution -> Desired Plan

1. Analysis - Desire state as apposed to current state

- 1.1 Stakeholder Engagement
- 1.2 Business & Technical Goals, design Analysis
- 1.3 Migration Constraints & Analysis
- 1.4 Migration Strategy

JUNIPER NETWORKS DESIGN ASSOCIATE

JN0-1102

2. Migration Plan

- Processes
- People
- Technology
- Tools
- Risk Mitigation
- Execution Plan

2.1 Migration Plan

2.2 Migration Acceptance Test Plan

2.3 Migration Validation Testing

3. Migration Execution

- Plan Execution
- Testing
- Refining
- Cutover

3.1 Pre-Migration Readiness

3.2 Migration Cutover

3.3 Post-Migration Acceptance Testing

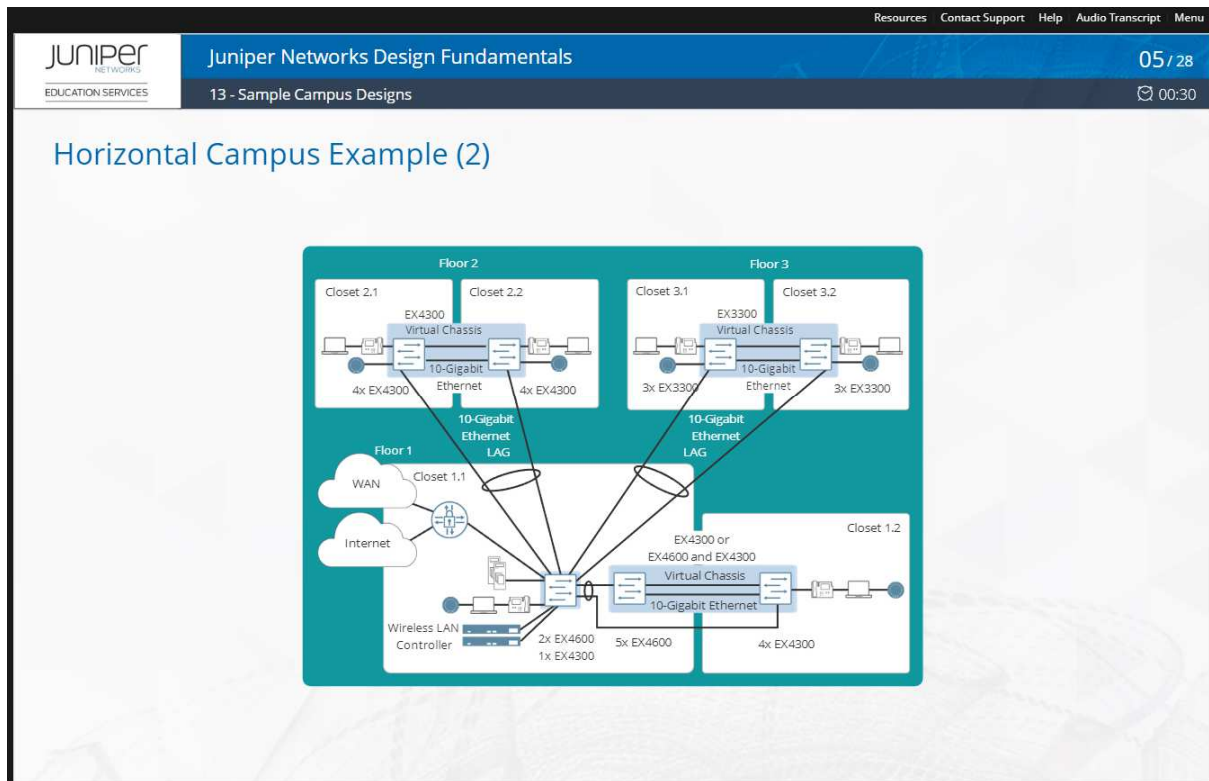
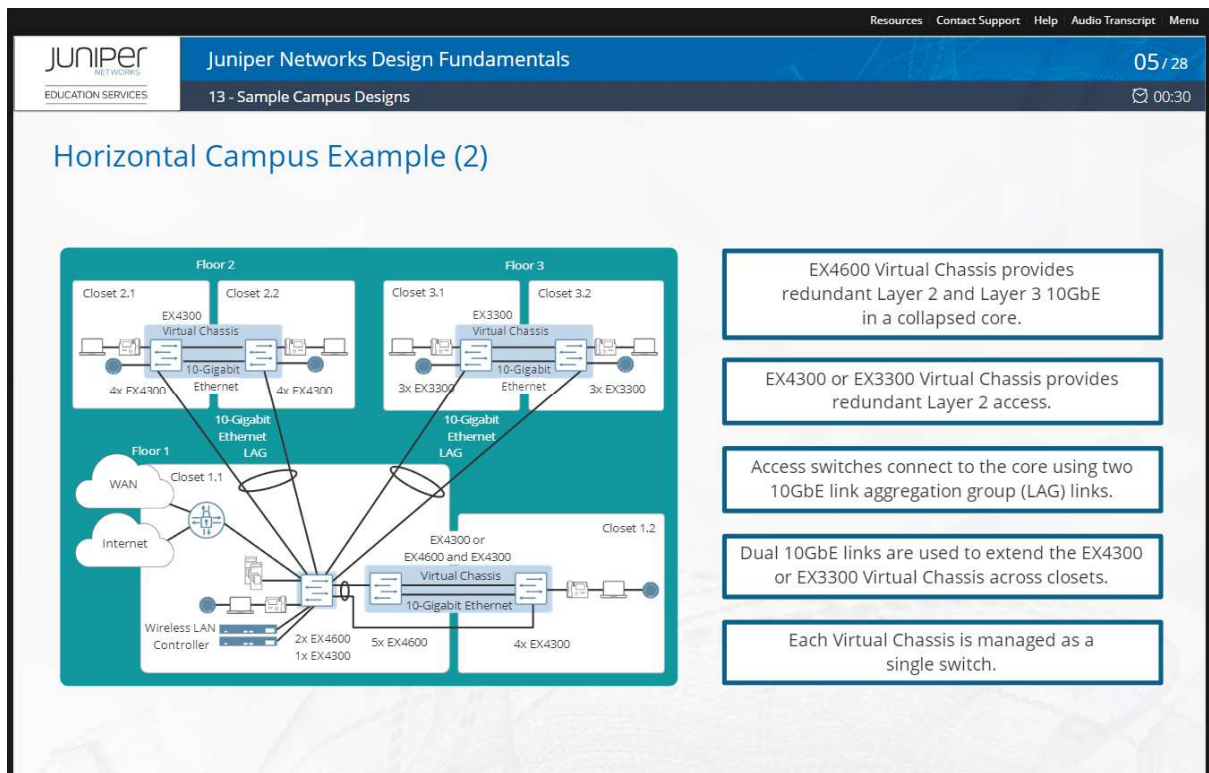
3.4 Migration Handover

Automation: Leveraged Across All Phases

- Automation scripts and tools
 - Help drive efficiency
 - Accelerate project delivery
 - Simplify migration workflows
 - Enable precision and promote accuracy
 - Mitigate risk

JUNIPER NETWORKS DESIGN ASSOCIATE JN0-1102

Appendix



JUNIPER NETWORKS DESIGN ASSOCIATE JN0-1102

Resources Contact Support Help Audio Transcript Menu



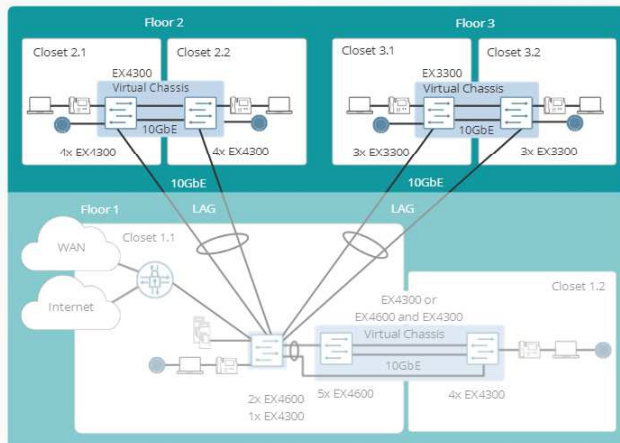
Juniper Networks Design Fundamentals

13 - Sample Campus Designs

06 / 28

00:33

Horizontal Campus Example (3)



Dual 10GbE links are used to extend the EX4300 or EX3300 Virtual Chassis across closets.

Each Virtual Chassis is managed as a single switch.

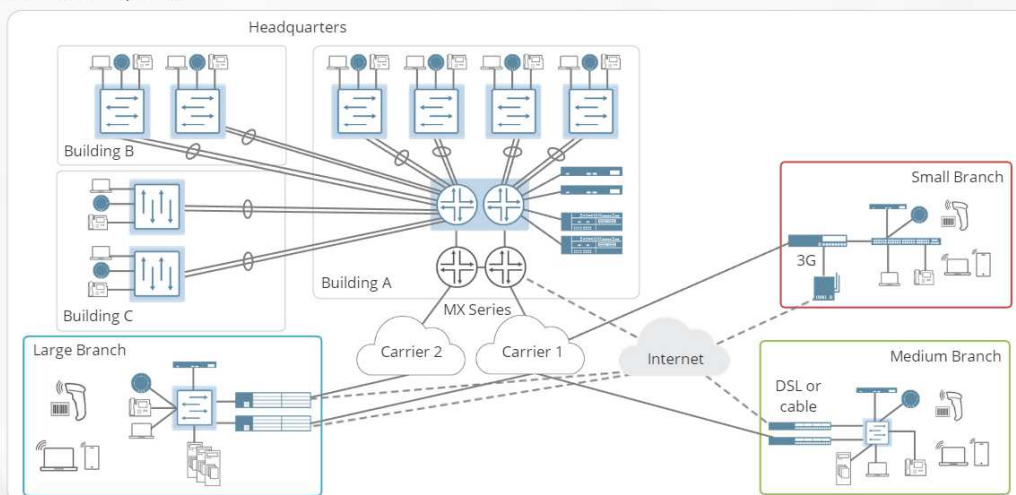
No blocked links.

No First Hop Redundancy Protocol (FHRP) (Virtual Router Redundancy Protocol (VRRP), Hot Standby Routing Protocol (HSRP), or global server load balancing (GSLB)).

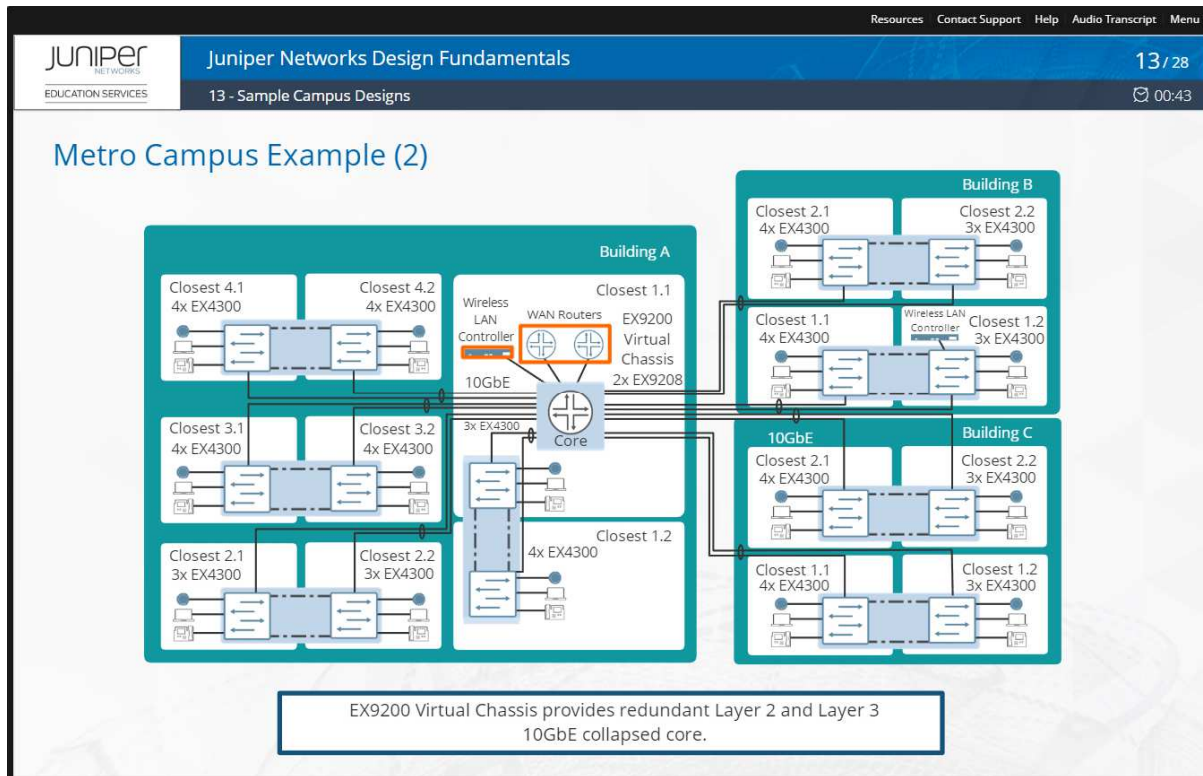
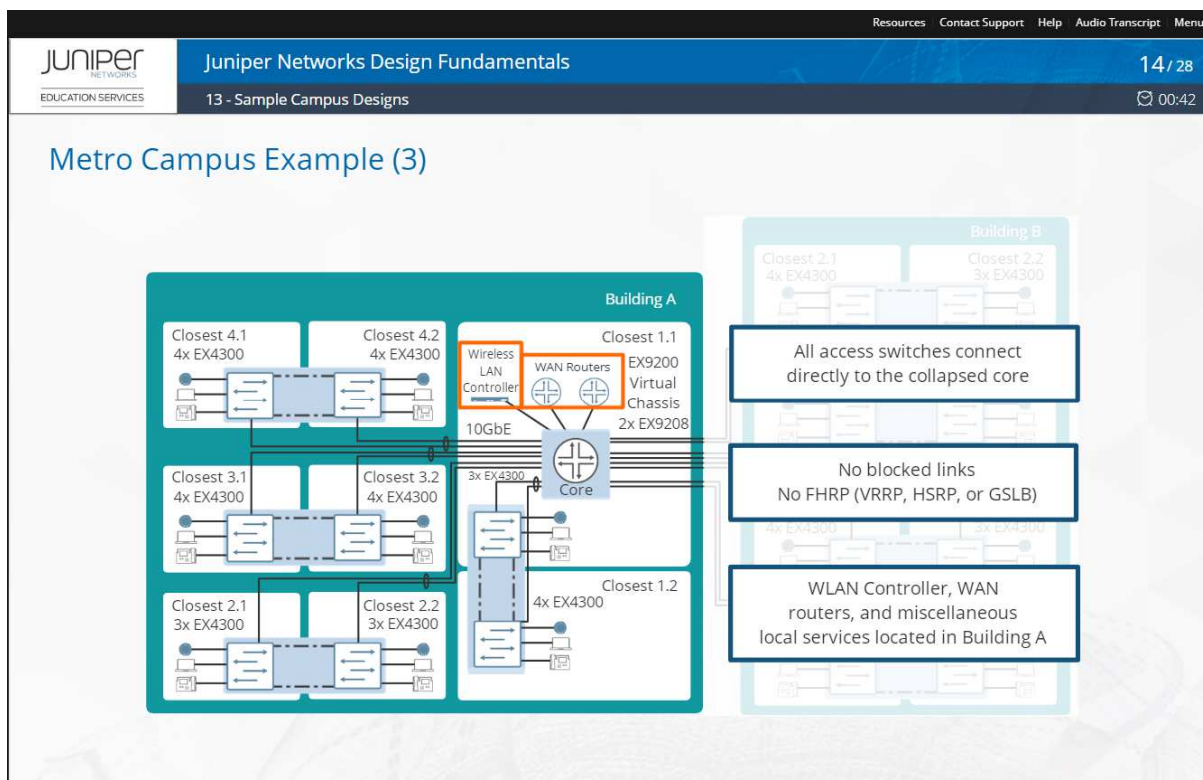
Hub and Satellite Campus Example (2)

Hub and Satellite Campus with Three Branch Sizes

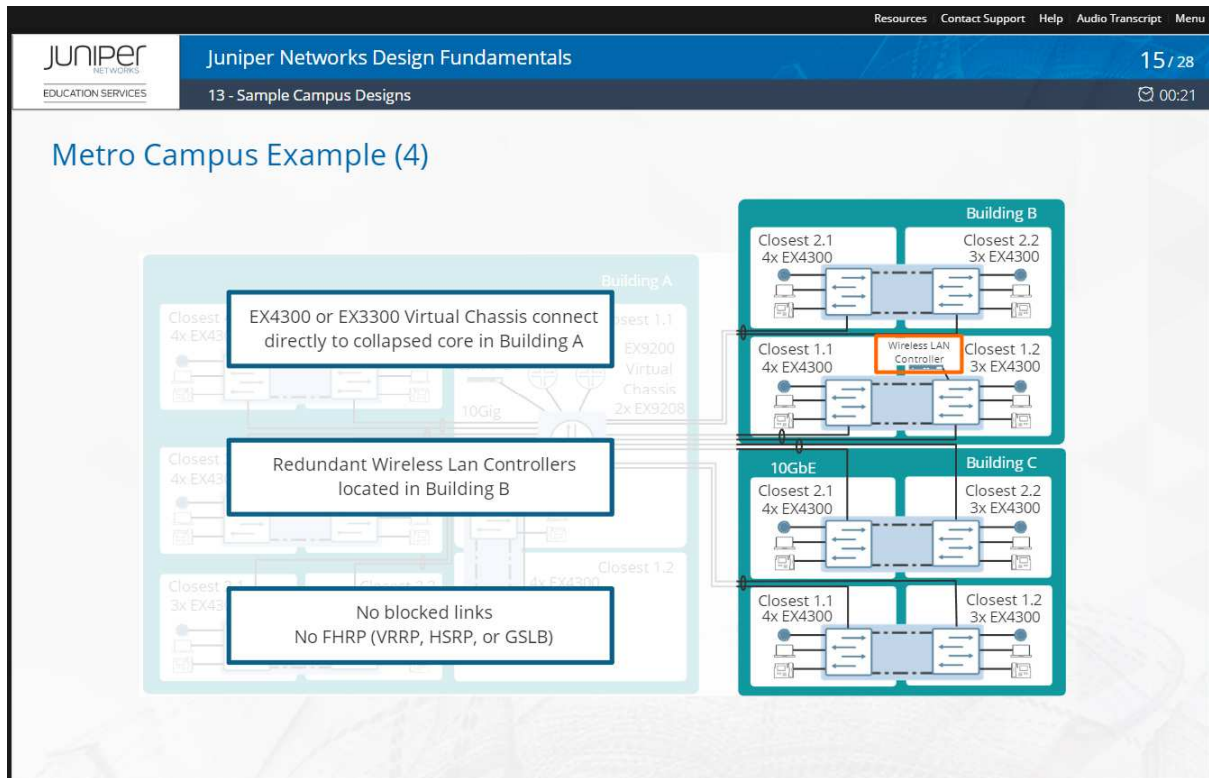
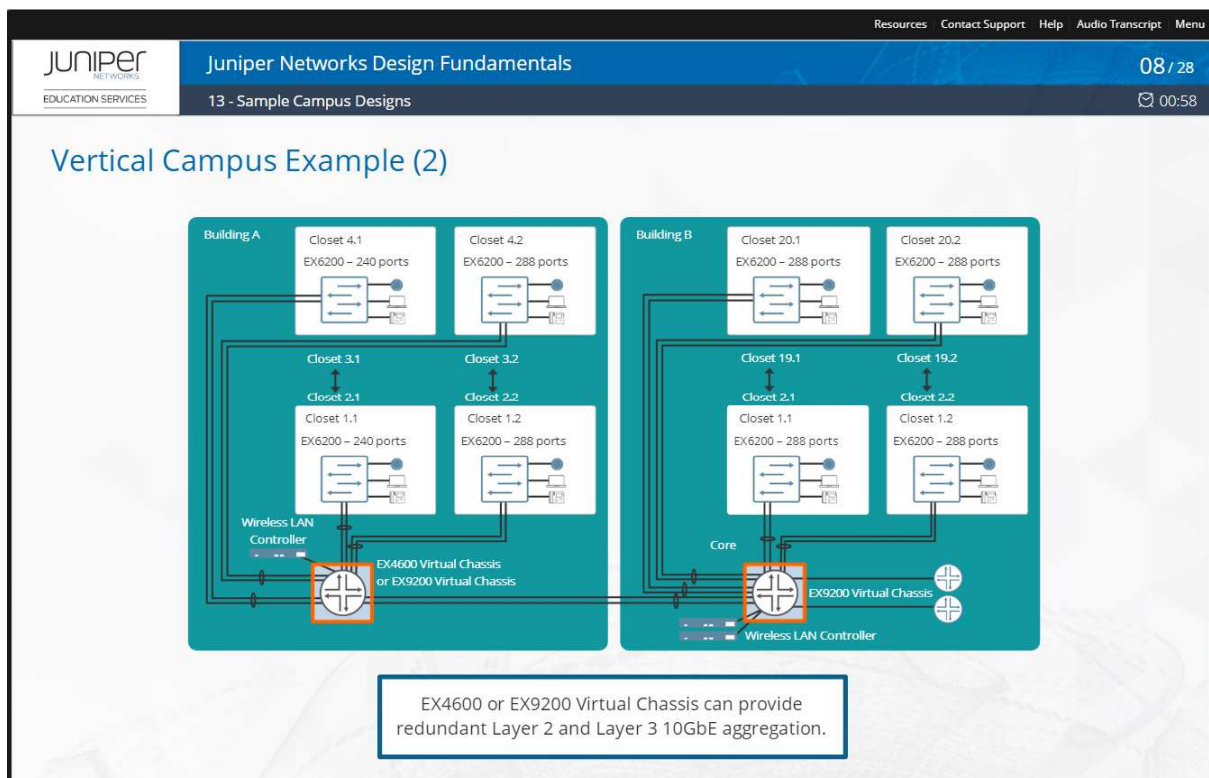
- Redundancy is used at the headquarters location where possible, and the large and medium branches take advantage of Virtual Chassis capabilities



JUNIPER NETWORKS DESIGN ASSOCIATE JN0-1102



JUNIPER NETWORKS DESIGN ASSOCIATE JN0-1102



JUNIPER NETWORKS DESIGN ASSOCIATE JN0-1102



JUNIPER

NETWORKS

EDUCATION SERVICES

Juniper Networks Design Fundamentals

13 - Sample Campus Designs

Resources

Contact Support

Help

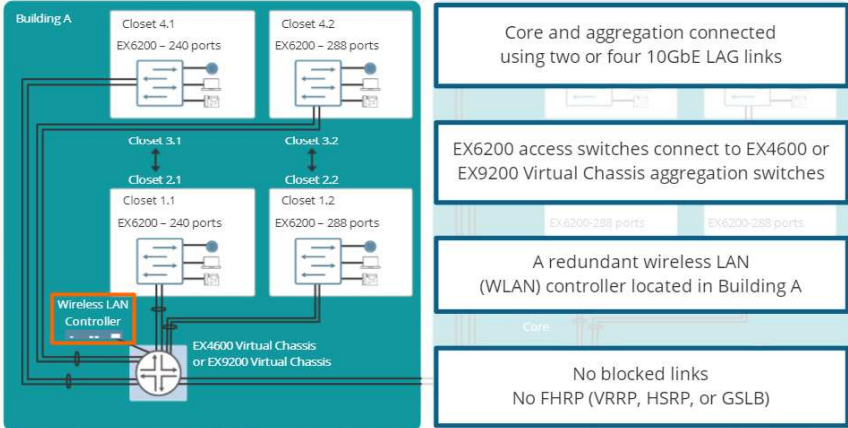
Audio Transcript

Menu

09 / 28

00:36

Vertical Campus Example (3)



The diagram illustrates a vertical campus design for Building A. It features a core and aggregation layer at the top, connected to a layer of EX6200 access switches. These access switches are connected to a layer of EX4600 or EX9200 Virtual Chassis aggregation switches. A Wireless LAN Controller is located in Building A, connected to the aggregation switches. The diagram shows a redundant wireless LAN (WLAN) controller. The core and aggregation are connected using two or four 10GbE LAG links. The access switches connect to the aggregation switches. The diagram also shows a redundant WLAN controller located in Building A. The core and aggregation are connected using two or four 10GbE LAG links. The access switches connect to the aggregation switches. The diagram also shows a redundant WLAN controller located in Building A. The core and aggregation are connected using two or four 10GbE LAG links. The access switches connect to the aggregation switches. The diagram also shows a redundant WLAN controller located in Building A.

Core and aggregation connected using two or four 10GbE LAG links

EX6200 access switches connect to EX4600 or EX9200 Virtual Chassis aggregation switches

A redundant wireless LAN (WLAN) controller located in Building A

No blocked links
No FHRP (VRRP, HSRP, or GSLB)



JUNIPER

NETWORKS

EDUCATION SERVICES

Juniper Networks Design Fundamentals

13 - Sample Campus Designs

Resources

Contact Support

Help

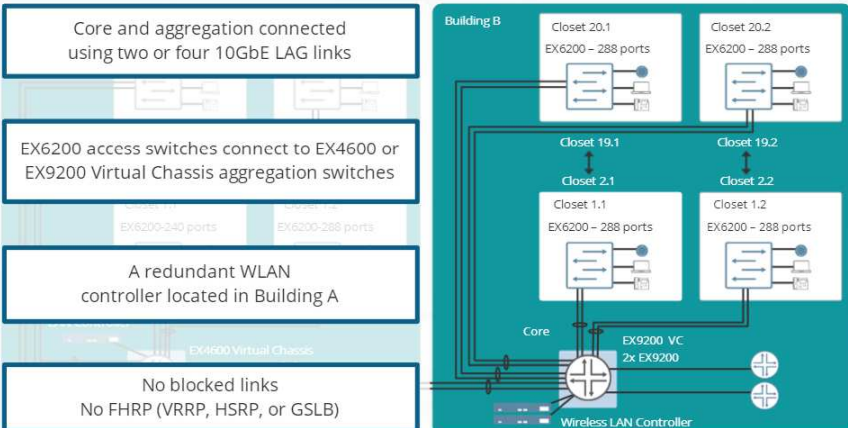
Audio Transcript

Menu

10 / 28

00:13

Vertical Campus Example (4)



The diagram illustrates a vertical campus design for Building B. It features a core and aggregation layer at the top, connected to a layer of EX6200 access switches. These access switches are connected to a layer of EX4600 or EX9200 Virtual Chassis aggregation switches. A Wireless LAN Controller is located in Building B, connected to the aggregation switches. The diagram shows a redundant wireless LAN (WLAN) controller. The core and aggregation are connected using two or four 10GbE LAG links. The access switches connect to the aggregation switches. The diagram also shows a redundant WLAN controller located in Building B. The core and aggregation are connected using two or four 10GbE LAG links. The access switches connect to the aggregation switches. The diagram also shows a redundant WLAN controller located in Building B. The core and aggregation are connected using two or four 10GbE LAG links. The access switches connect to the aggregation switches. The diagram also shows a redundant WLAN controller located in Building B.

Core and aggregation connected using two or four 10GbE LAG links

EX6200 access switches connect to EX4600 or EX9200 Virtual Chassis aggregation switches

A redundant WLAN controller located in Building B

No blocked links
No FHRP (VRRP, HSRP, or GSLB)

JUNIPER NETWORKS DESIGN ASSOCIATE JN0-1102



Juniper Networks Design Fundamentals

13 - Sample Campus Designs

Resources

Contact Support

Help

Audio Transcript

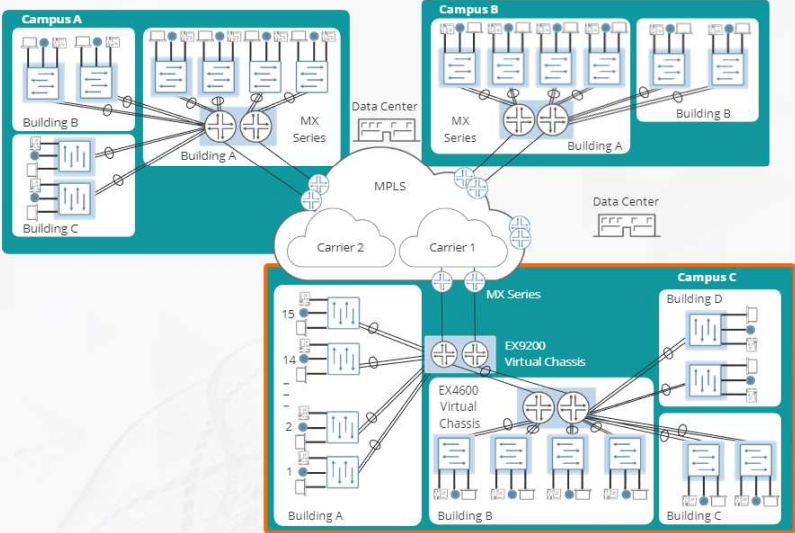
Menu

17 / 28

00:16

Widely Distributed Campus Example (2)

Widely distributed campus with MPLS core





Juniper Networks Design Fundamentals

13 - Sample Campus Designs

Resources

Contact Support

Help

Audio Transcript

Menu

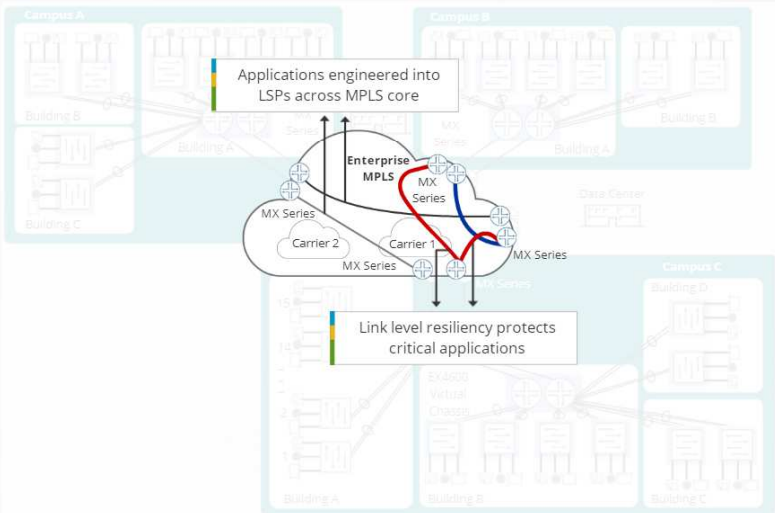
20 / 28

00:35

Widely Distributed Campus Example (5)

MPLS Provides Segmentation Between Multiple Sites

- The MPLS cloud consolidates data transport



Applications engineered into LSPs across MPLS core

Enterprise MPLS

Link level resiliency protects critical applications