# IP Network

LAN/WAN Fundamentals

# ACKNOWLEDGEMENT

This lecture material was developed with primary references to:

**Cisco Smart Business Architecture**

While the focus of this lecture is on the fundamentals of internetworking, some of the concepts provided here are exclusively owned by Cisco SBA, its purpose is to shift the idea from the older and convoluted to the newer and simplified technology and business approaches.

Disclaimer: They may not be responsible to the accuracy of this material.

# Internetworking fundamentals

- OSI & TCP/IP models
- IP addressing modes
  - IPv4
  - IPv6
- Routing basics and functions

# Argument related to internetworking

- Simple plumbing
  - Size and length of the pipes
  - Speed and feeds of the links
- Complex plumbing i.e. large stadium, high rise buildings
  - Scale
  - Purpose
  - Redundancy
  - Protection
    - Tampering, denial of service
  - Capacity to handle peak loads

# Rationale

- Access from users with their
  - Information, doing their jobs
  - Transport of voice (VoIP) and video (video conferencing)
- Reliability and resiliency
- Intelligent, fault-tolerant transport and load sharing decisions
- Performance sensitive
  - Prevent delays (latency), jitter and packet loss

# LAN

- Wired
  - Primary connectivity for local users
  - Core for interconnecting the WAN, data center, server rooms
  - Internet access
- Large LANs and campus networks
  - Require a high-availability design
  - Support mission critical applications
  - Real-time multimedia communications
- Drives organizational operations
- Business-enabler

# LAN continuation

- In many LAN designs
  - Redundancy
  - Resiliency
    - Stay in backup status and remain unused or in standby mode

# LAN hierarchical design

- Core layer
  - Provides users/workgroups access to the network
- Distribution layer
  - Aggregates access layers and provides connectivity to services
- Access layer
  - Provides connection between distribution layers for large LAN environments

# LAN access layer

- User-controlled and user-accessible devices connect to the network
- Provide formerly expensive, high-speed connectivity (GbE) or wireless as standard configuration
- Plays important role in protecting users, application resources, and the network itself from human error and malicious attacks
- Strictly restrict unauthorized users
- Prevent attempt to takeover the role of any other device on the network
- Verify devices that are allowed on the network

# LAN access layer continuation

- Provides automated services
  - Power over Ethernet (PoE)
  - VLAN assignments
    - IP telephone, reduces operational requirements
    - Span multiple access layer closets to satisfy an application requirement
- Enabling advance technology capabilities i.e. video and voice

# Connectivity: LAN access layer

- Devices to connect
  - Personal computers
  - Smartphones
  - Wireless access points
  - IP video and surveillance cameras
- Support many logical network on one physical infrastructure (check page 7 for access layer connectivity with the deployment guide)

# Security: LAN access layer

- Ensures that the network is available for use without impairment for everyone that needs it
- Prevents attempt to takeover the role of any device on the network
- Verifies allowed devices
- Contributes to resiliency and availability

# Security features: LAN access layer

- DHCP snooping, tracks
  - MAC addresses
  - IP address lease time and binding type
  - VLAN number
  - Interface info that corresponds to the local untrusted interfaces in the switch
  - Stores the preceding information
    - DHCP binding table
  - Blocks DHCP replies on an untrusted interface

# Security features: LAN access layer continuation

- Port security
  - Limits the number of MAC addresses that can be in a single port
    - Prevents MAC flooding
  - Secure MAC addresses
    - Allow inbound traffic from only a restricted set of MAC addresses, this lets you configure L2 interfaces
    - Does not allow traffic from these MAC addresses on another interface within the same VLAN

# Security features: LAN access layer continuation

- Dynamic ARP inspection
  - Mitigates ARP poisoning attacks
    - Sending of false ARP information to a local segment
      - Designed to poison the ARP cache of devices on the LAN
      - Allows attacker to execute MITM attacks
- Uses data generated by the DHCP snooping
- Intercepts and validates the IP-to-MAC address relationship of all ARP packets on untrusted interfaces

# Security features: LAN access layer continuation

- IP Source Guard
  - Prevents a packet from using an incorrect source IP address
    - Obscure it source, also known as IP spoofing
  - Uses information from DHCP snooping to dynamically configure a port access control list (PACL) on the interface that denies any traffic from IP addresses that are not in the DHCP binding table

# LAN distribution layer, older mechanism

- Serves primarily as an aggregation point
- First point of IP layer 3 services
  - Packet switching
  - Routing
- Requires high availability design
  - Traditionally results in complex interconnection of redundant links as well as protocols
    - Spanning Tree Protoocols (STP)
    - First Hop Routing Protocols (FHRP)
      - Manages availability and path selection
  - Creates a loop that STP detects and mitigates by shutting down one of the redundant uplinks
    - To prevent loops which causes to reduce usable bandwidth
    - The active STP loop avoidance can be much slower to recover from link outages by unblocking redundant uplinks
    - Can be error prone when misconfigured, misuse of subjected to one-way communication failures

# LAN distribution layer, newer mechanism

- Improves traditional design using resilient virtual switch design
- Provides, via virtual switch design, device redundancy by making 2 physical switches appear as a single switch or stack with redundant logic and power
- EtherChannel and MultiChassis EtherChannel allow active forwarding of redundancy access layer uplinks
  - Provides sub-second failover for failed links and eliminate bridging loops and associated STP blocked interfaces
  - Eliminates FHRPs reduces the complexity of the configuration by over 50%
  - Makes network easier to troubleshoot and fast recovery in the event of failures
- Forwards traffic without creating dangerous L2 loops in the network
- The best benefit for a company, reduce operational expenses

# Scalability: LAN distribution layer

- Serve end user connectivity
- Provide logical point to summarize addressing
- Create boundary for protocols and features necessary for the access layer operation
- Creates fault domains to contain failures or network changes to those parts of the network directly affected
  - Increases network availability
- Lowers cost of operation by making it more efficient—requiring less memory and processing resources for devices elsewhere in the network

# Resiliency: LAN distribution layer

- Reduces complexity of configuration and operation as fewer protocol are required and little or no tuning is needed
  - Provides near-second or sub-second convergence around failures or disruptions
- Provides physically redundant components
  - Power supplies
  - Supervisors
  - Modules
  - Stateful switchover to redundant logical control planes

# Flexibility: LAN distribution layer

- Provides connectivity to
  - Network-based services
  - WAN
  - Internet edge
- Aggregates LAN access layer connectivity
- Referred to as the “collapsed core”
  - Distribution layer serves as the L3 aggregation layer for all devices

# LAN design require dedicated (and larger) distribution layer

- WAN routers
- WAAS controllers
- Internet edge devices
- WLAN controllers

# Factors drive LAN multi-distribution layer modules

- Network performance and throughput
  - Number of ports and port speed
- Network resilience
  - All LAN rely on single platform
  - Present of single point of failure or unacceptably large failure domain
  - Change control and frequency can affect the entire network
- Fiber optic interconnects back to the single collapsed core
  - Geographic dispersion of LAN access switches across many buildings or larger campus facility
- QoS, like the access layer
  - Guarantee critical and multimedia application flows

# Distribution layer deployment

- Traditional distribution layer design
  - Deploys a multitier approach with L2 from the access layer to the distribution layer where the L2 boundary exists
- Connectivity to the access to the distribution layers can result in either
  - Loop free
  - Looped design
- Design has 2 standalone switches for resiliency
  - Unrestricted L2 VLAN cause STP to block, common point of failure in LANs
  - Restricted VLAN to a single switch provides a loop free, does limit network flexibility

# LAN core layer

- Provides aggregation when multiple distribution layer exist in a single, collocated topology and is designed to use only point-to-point L3 IP-routed links
- Migrates naturally from a smaller two-tier network to a larger three-tier network
  - Utility maybe distinct with big companies, campuses and ISPs
- Serves scalability requirements and serves as critical part and feature of network
- Has 24*7*365 design criteria, the highest possible availability
- Eliminates high complexity or should avoid running high touch services in order to reduce outages, planned of unplanned
  - Configuration changes
  - Maintenance

# LAN core layer continuation

- Developed with the existence of multiple distribution layer switches
- Access layer switches are located in multiple geographically dispersed building
  - Fiber optic runs may be reduced by connecting directly distribution layer switches
- Required when distribution layer grows beyond 3 in a single location
  - Multiple distribution layer is created when the performance required in the access layers exceeded the original network design
  - Optimize and seamlessly adjust the design

# LAN core layer continuation

- Represents the 24*7*365 non-stop connectivity
- The conduct business is critical
- Connectivity to and from the core is L3
  - Drives increase resiliency and stability
- Especially relevant to design where the data center resources might be collocated with the LAN
- Serves as the connection between WAN and Internet Edge distribution blocks
- Central point of connectivity of all data flows
- Part of the backbone IP routing address space
- Designed to be highly resilient to protect from
  - Component-induced outage
  - Power-induced outage
  - Operation-induced outage

# LAN core layer continuation

- Built on dual switches
  - Provide a separate control plane (check succeeding slide) housed on each switch which provides (for the backbone operation)
    - Redundant logic
    - Line cards
    - Hardware
    - Power
- Distribution layer block should be dual homed with an EtherChannel or link to each core switch
  - Provides Equal Cost Multi Path (ECMP) – load sharing of IP traffic across links for traffic traversing the core
  - Provides fast failover based on EtherChannel or ECMP alternate routes without waiting for routing protocol topology changes to propagate the network

# LAN core layer continuation

- Designed to be high speed
- Provides connectivity ranging from
  - Gigabit Ethernet to 40 GbE
  - Gigabit EtherChannel to 40 GbEC
  - Non-blocking blocking bandwidth based on design and configuration

# Core: Control and forwarding planes

- Control plane – the part of the router architecture that is concerned with drawing the network map, or the information in a (possibly augmented) routing table that defines what to do with incoming packets
  - Make preferential treatment of certain packets for which a high quality of service is defined by such mechanisms as differentiated services
  - A major function is deciding which routes go into the main routing table
- Forwarding plane - sometimes called the **data plane**, defines the part of the router architecture that decides what to do with packets arriving on an inbound interface
  - it refers to a table in which the router looks up the destination address of the incoming packet and retrieves the information necessary to determine the path from the receiving element, through the internal **forwarding fabric** of the router, and to the proper outgoing interface(s)

# QoS: LAN core layer

- Special handling of real-time traffic, sensitive to delay and drop
  - UDP applications
    - Audio and video
    - Deterministic handling of such traffic
- Useful in congestion handling
- Takes bandwidth from one class to give priority to another class
  - Does not create bandwidth

# QoS primary goals, LAN core

- Support and ensure first out-the-door service
- Provide business continuance
- Provide fairness between all other applications when congestion occurs
- Build a trusted edge around the network
  - Guarantees users not to inject their own arbitrary priority values
  - Allow to trust marked traffic throughout the network

# QoS steps approach to accomplish goals, LAN core

- Establish a limited number of traffic classes
  - The need for special handling i.e. real-time video, voice et al
- Classify applications into traffic classes
- Apply special handling to traffic classes
  - Achieve intended network behavior

- Establishes a solid, scalable and modular framework

# LAN design models

- Single-tier LAN
- Two-tier LAN
- Three-tier LAN

# Single-tier LAN design model

- Utilizes single access layer switch for
  - Wired user access
  - WAN router
  - Wireless LAN access point connectivity
  - Same access layer functions provided in larger sites can be applied
    - Power over Ethernet
    - Quality of Service
    - Security

# Two-tier LAN design model

- Provides an aggregation point for connecting all of the wirings of various offices
- The distribution layer may function as a collapsed core making centralized connectivity for
  - Access layers
  - WAN routers
  - Data center and/or server room
  - Internet edge

# Three-tier LAN design model

- Adds core layer to aggregate multiple distribution layers
- Accommodates large number of access layers spread over multiple floors
- Separates services distribution layer provides
  - Supports modular growth for high densities of WAN head end routers and WAN services
  - Wirelss LAN controller termination in a central location of a larger campus populations
  - Fault domains separate from the LAN access for a more resilient network
  - IP address summarization from WAN or Internet edge toward the core of the network

See figure about scalable architecture to meet multiple requirements, page 3 with Deployment Guide, Feb2013

# Wireless LAN

- Benefits
  - Improves the effectiveness and efficiency of employee, regardless of location
  - Integrated part of wired-network design
  - Hard-to-wire locations can have connection
  - Centralized control of distributed wireless environment is easy to manage and operate
  - Wireless network core is a plug-and-play deployment

# 1G Wireless LAN

- Unsecure
- Difficult to manage
  - Autonomous, which proved to be a non-scalable deployment and operation model
- Traditional and stand-alone access point model costly, though considered secure at headquarters and remote sites

# NG Wireless LAN

- Centralized management regardless of the number of APs dispersed
- Secure access to wireless LANs
- User authentication in a corporate directory service
- Grant guest access while separating their traffic
- Enables
  - Load balancing
  - Scalable
  - Redundancy
    - Important especially during maintenance and unexpected outages

# Cisco Unified Wireless Network

- Local mode
  - LAN controller is connected to the distribution layer
  - Wireless LAN controller and APs are co-located
  - Traffic between wireless LAN clients and LAN is tunneled in Control and Provisioning of Wireless Access Points, between controller and AP
  - Uses the controller as a single point for managing L2 security and wireless network policies
- Flex connect
  - Utilize for remote deployments
  - Controller is not necessary in remote site as it can be utilized through WAN

# Cisco Unified Wireless Network continuation

- Local mode
  - Support customer demands including
    - Seamless mobility
    - Ability to support rich media
    - Centralize policy
  - Site has LAN distribution layer
  - Site has >50 APs
  - Site has WAN latency greater than 100ms to a proposed shared controller
- Flex connect
  - Site LAN is a single access-layer switch or stack
  - Site has <50 APs
  - Site has WAN latency less than 100ms round trip to the shared controller

# Flex Connect deployment

- APs switch wireless traffic onto the wired interface
- WLAN segmentation is maintained using IEEE 802.1Q trunking
  - Separates multiple WLANs for transportation on the wired infrastructure
- Can tunnel guest wireless traffic back tot the centralized controller

# Guest and partner wireless access

- When productivity is crucial
  - Guest access should be throughout the network
- With existing infrastructure without having to add another for the guest and partner's reduces cost and complexity
- Secure transport keeps guest traffic segmented from the internal network
- Guest access is controlled by IT
  - Administrative staff can grant access request for guests

Check page 15 figure, Design Overview, Feb2013