Technologies used and future technologies.

This outline will list what technologies are used in our network infrastructure. After the completion of this training JCU members will have the oppurtunity in lieu of SONOC (RIP) to have a deeper understanding of the networking technology we use, and how we utilize it in our enterprise. Looking towards the future, at the end of this training I will go over Cisco SDN technologies and also Cloud-based networking infrastructure (Azure).

1. **VLANs** -- Virtual Local Area Networks are used to segment traffic in our local environments
    - 802.1q encapsulation
    - Trunking, VLAN pruning, static trunks
    - Private VLANs
    - SVIs
2. **BDIs** -- Bridge Domain interfaces
3. **etherchannel** -- Etherchannel is the Cisco technology that does link aggregation and improves bandwidth on L2/L3 links.
    - Layer 2 LACP
    - Layer 3 LACP
    - VSS/Stackwise
4. **DHCP** -- Dynamic Host Control Protocol
    - iOS Configuration
    - DHCP pools for VRFs
    - DHCP exclusion
    - IP helper-address (DHCP Relay)
    - DHCP options (150, 66, 67)
5. **Layer 2 Security** -- Our enterprise employs security control at layer 2 to protect our enterprise
    - NAC/802.1x (overview not configuration)
    - DHCP Snooping
    - Blackhole VLANs
    - Dynamic ARP inspection
6. **Key Chains** -- Key chains are used for network authentication between control plane protocols like - OSPF, EIGRP, NTP
    - key chain configuration
    - rolling keys
    - lifetimes
7. **ACLs** -- Access Control Lists identify traffic to be filtered, distributed, or used in QOS/ZBF.
    - Standard ACLs
    - Extended ACLs
    - Named ACLs
    - Editing ACLs
    - Applying ACLs to different interfaces (VTY, ethernet)
    - Using ACLs to identify traffic in policiing policies (QOS), or redistribution

8. **NTP** -- Network timing protocol is essential when employing security controls like authentication for EIGRP. Timing must be synchronized across an enterprise.
   - Stratum levels
   - NTP iOS configuration
   - NTP authentication
   - setting clock manually
9. **AAA** -- Authentication, Authorization, and Acccounting. AAA is used in networking to employ TACACS, and RADIUS technologies for Network Access Control (NAC), and to integrate iOS devices into Cisco's Identity Services Engine (ISE)
   - AAA overview
   - TACACS authentication/authorization/accounting iOS configuration
   - RADIUS iOS configuration for 802.1x
10. **EIGRP** -- EIGRP is the IGP we use to route enclave traffic.
    - DUAL Algorithm
    - How Neighborship forms, adjaceny, and topology table
    - EIGRP rules for neighborship (Hello/hold timers, AS #)
    - Network command
    - Stub routing
    - passive-interfaces
    - EIGRP Authentication
    - Leak-maps | distribute lists
    - Metric tuning (offset lists)
11. **VRF** -- Virtual Route Forwarding is how we create virtual routing tables that are segmeneted logically from the global routing table
    - VRF overview and use case (JSOC Enterprise specific)
    - VRF iOS configuration
    - Applying an interface to a VRF
    - Applying a VRF to routing protocol
12. **QOS** - Quality of Service is used for control plane policing, identifying, marking and classifying traffic, and can be used in degraded environments to prioritize mission essential traffic
    - QOS overview (DCSP, TOS, COS)
    - QOS methods (marking, classifying, policing, queing, shaping)
    - Cisco Common Classification policy language (CP3L), class-maps, policy-maps, service-maps
    - Applying QOS to interfaces, CoPP, and DMVPN tunnels
13. **ZBF** - Zone based firewalls are used in Cisco iOS to segment and separate traffic on a single router
    - ZBF overview (inside, outside, self)
    - ZBF configuration C3PL
    - Applying the zones
14. **IPSEC** -- Internet Protocol Security is a encryption technology that is used for VPNs and employs authentication, confidentiality, and non-repudiation for your data traffic
    - VPN overview
    - ISAKMP overview
    - Internet Key Exchange over (IKEv1, IKEv2)
    - IPSec iOS configuration
    - Applying IPSEC to interfaces

15. **DMVPN** -- Dynamic Multipoint VPN is a Hub-and-spoke topology used in Cisco devices to create dynamic VPNs using an NBMA and NHS address. (Underlay/overlay)
    - DMVPN configuration
    - Phase 2 / 3 configuration
    - Per QOS tunneling on DMVPN
    - IPSec on DMVPN
16. **FLEXVPN** -- FlexVPN is another VPN technology that can be used in a hub-and-spoke topology
    - FlexVPN overview (pros and cons, FLexVPN vs DMVPN)
    - FlexVPN configuration using PSK
    - FlexVPN Hub show commands
17. **prefix-lists** - IP Prefix-lists are another way to identify traffic and be used to filter traffic
    - Prefix-list overview (pros and cons, prefix-list vs ACL)
    - prefix-list iOS configuration
18. **route-maps** -- Route maps are used in Cisco iOS for routing policy and can be used for leak-maps and distribute lists in routing protocols
    - Route-map overview
    - Route-map configuration
19. **redistribution** -- Routing protocol redistribution allows multiple routing protocols to share routes with each other
    - Redistribution overview (why and where we use it)
    - OSPF--BGP configuration
    - EIGRP--OSPF configuration
    - EIGRP--BGP configuration
20. - **OSPF** - Another IGP we use as the underlay for our Core/transport network
    - Single area
21. **BGP** -- This is the exterior gateway protocol used to share routes between autonomus systems and our core transport network.
    - BGP overview (IGP vs EGP, Autonomous systems, how BGP is an application)
    - BGP metrics/weights
    - iBGP configuation
    - eBGP configuation
    - route reflector configuration
22. **MPLS** -- Multi protocol label switching is a networking technology that uses "labels" to route traffic and is used to traffic engineer our transport network
    - MPLS overview (why we use it, layer 2 vs layer 3, MPLS L3 VPN)
    - TE tunnels
    - OSPF underlay
    - RSVP
    - LDP
23. **SNMP** -- Simple Network Management protocol is a network application protocol that is used to pull information and map our network
    - SNMPv3 configuration
24. **applets** -- EEM applets are triggered code that is used to dynamically apply configuration without administrator intervention
    - Applet overview (how and why we use them in our enterprise)
    - Applet configuration

25. **SD-WAN** -- SD-WAN is a SDN based technology that uses Cisco vDevice infrastrcure to centralize network routing by using policies and consistent configuration
    - SD-WAN overview and why we would use it over MPLS
    - SD-WAN hardware constraints
    - SD-WAN devices, vAppliances
    - SD-WAN route policies and configuration
26. **SD-ACCESS** -- SD-Access is a SDN technology that can be used to centralize the control plane of network infrastructure
27. **Azure networking** -- Cloud networking is a new way to route traffic through a cloud based infrastructure using VPCs and Cloud data centers
    - VPCs
    - Public Cloud network infrastructure