ICX Workshop

Agenda

- ICX CLI Configuration
- Best Practices
- Questions?
- Reference Material

CLI Configuration

Accessing the Switch CLI

- Console and SSH/Telnet
  - Good free program to use is Putty:
  - http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

- TFTP
  - Good free program is TFTPD32
  - http://tftpd32.jounin.net/tftpd32_download.html

Internal Makeup

- Startup configuration
  - Configuration stored in flash that is used when the switch boots up
- Running configuration
  - Configuration stored in RAM that is used to run the functions of the switch in real time
- ***Write all configuration changes from running-config to startup-config or they will be lost on reboot!!***

- Primary and Secondary Flash
  - Location on switch where code images are stored. Boot is from primary by default.

Verification Commands

- show run
  - Show the running configuration of the system
- show configuration
  - Shows the startup configuration of the system
- show version
  - Shows the current boot and code images running on the system
- show flash
  - Shows the content of the primary and secondary flash partitions

Code Images

08030ga.zip

- FCX
- FSX
- ICX64xx
- ICX6610
- ICX6650
- ICX7250
- ICX7450
- ICX7750
- FI08030ga_Manifest.sig
- FI08030ga_Manifest.txt
- md5checksum.txt

- Boot
- Firmware
- Images
- MIBs
- Signatures

- SPR08030ga.bin
- SPS08030ga.bin

Ruckus™

Software Upgrades

- Boot Rom
  - Boot rom is the initial software to run the base hardware functions of the switch.
  - copy tftp flash 10.0.0.1 spz10105.bin bootrom

- Code Image
  - Software that runs all switching and routing functions (operating system)
  - copy tftp flash 10.0.0.1 SPS08030ga.bin primary

Software Upgrades

- Manafest.txt
  - Used to determine switch type and upgrade boot and image
  - Determines code type from what is already in Primary Flash

  - copy tftp system-manifest 10.0.0.1 FI08030ga_Manifest.txt primary

Code Images

- Switch Code
  - SPS08030ga.bin
- Route Code
  - SPR08030ga.bin

Defines code type (Switch or Route)

Defines code version

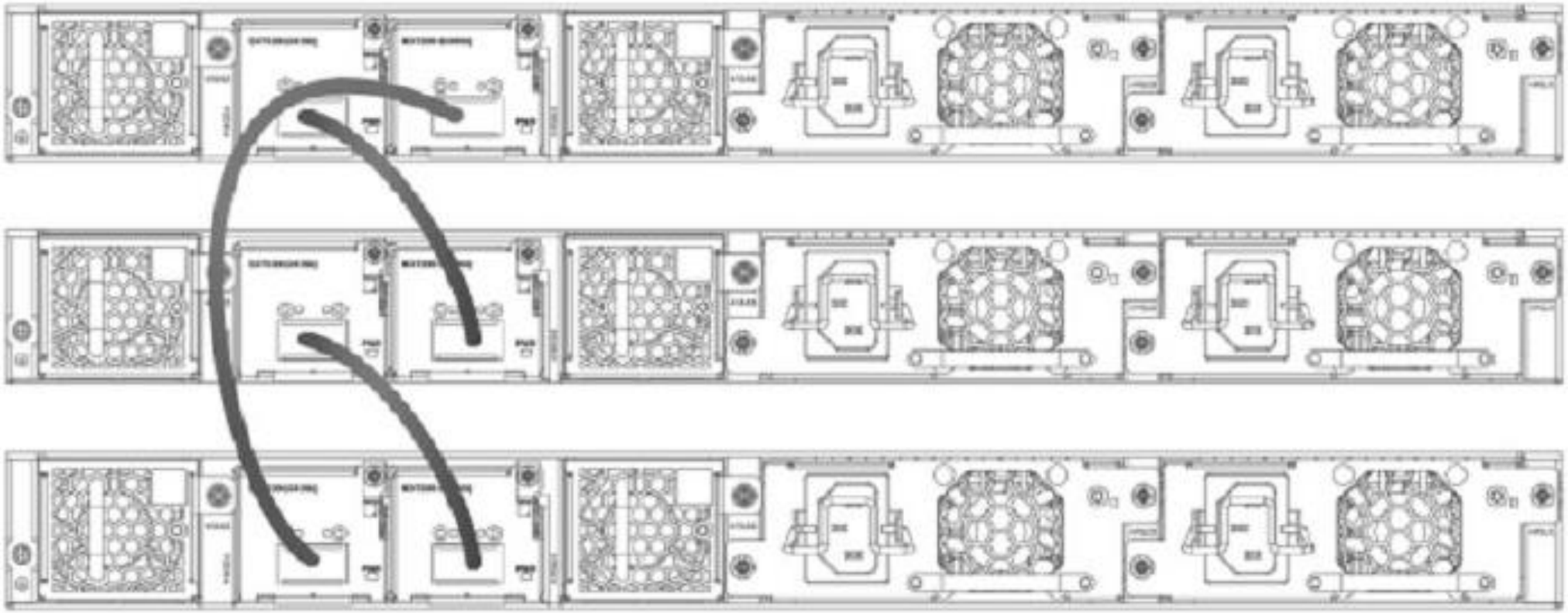
Stacking

- show stack
  - Shows the current stack topology
- stack enable
  - Enables stacking on the switch
- stack secure-setup
  - Configures stacking on connected units

- ***Switches must be on the same minor code revision to stack.***

Stack Cabling

FIGURE 20 ICX 7450 ring stack



Ruckus™

Stacking

- On the primary switch:
  - config t
  - stack enable
  - hitless-failover enable
  - exit
  - stack secure-setup
- When complete:
  - show stack

```
SSH@Lab-7450#show stack
T=1d1h41m25.7: alone: standalone, D: dynamic cfg, S: static
ID   Type           Role    Mac Address    Pri State   Comment
1  S ICX7450-24G    active  cc4e.2488.7cc8 128 local   Ready
2  S ICX7450-24G    standby cc4e.2488.7fc0   0 remote  Ready

    active       standby
     +---+        +---+
 -4/1| 1 |3/1--3/1| 2 |4/1-
  |   +---+        +---+   |
  |                        |
  |------------------------|
Standby u2 - protocols ready, can failover
Current stack management MAC is cc4e.2488.7cc8
SSH@Lab-7450#
```

Ruckus™

Stacking Configuration

```
stack unit 1
  module 1 icx7450-24-port-management-module
  module 2 icx7400-xgf-4port-40g-module
  module 3 icx7400-qsfp-1port-40g-module
  module 4 icx7400-qsfp-1port-40g-module
  priority 128
  stack-port 1/3/1 1/4/1
stack unit 2
  module 1 icx7450-24-port-management-module
  module 2 icx7400-xgf-4port-40g-module
  module 3 icx7400-qsfp-1port-40g-module
  module 4 icx7400-qsfp-1port-40g-module
  stack-port 2/3/1 2/4/1
stack enable
stack mac cc4e.2488.7cc8
!
```

- Consult the Switch Stacking Guide for more information.

Ruckus™

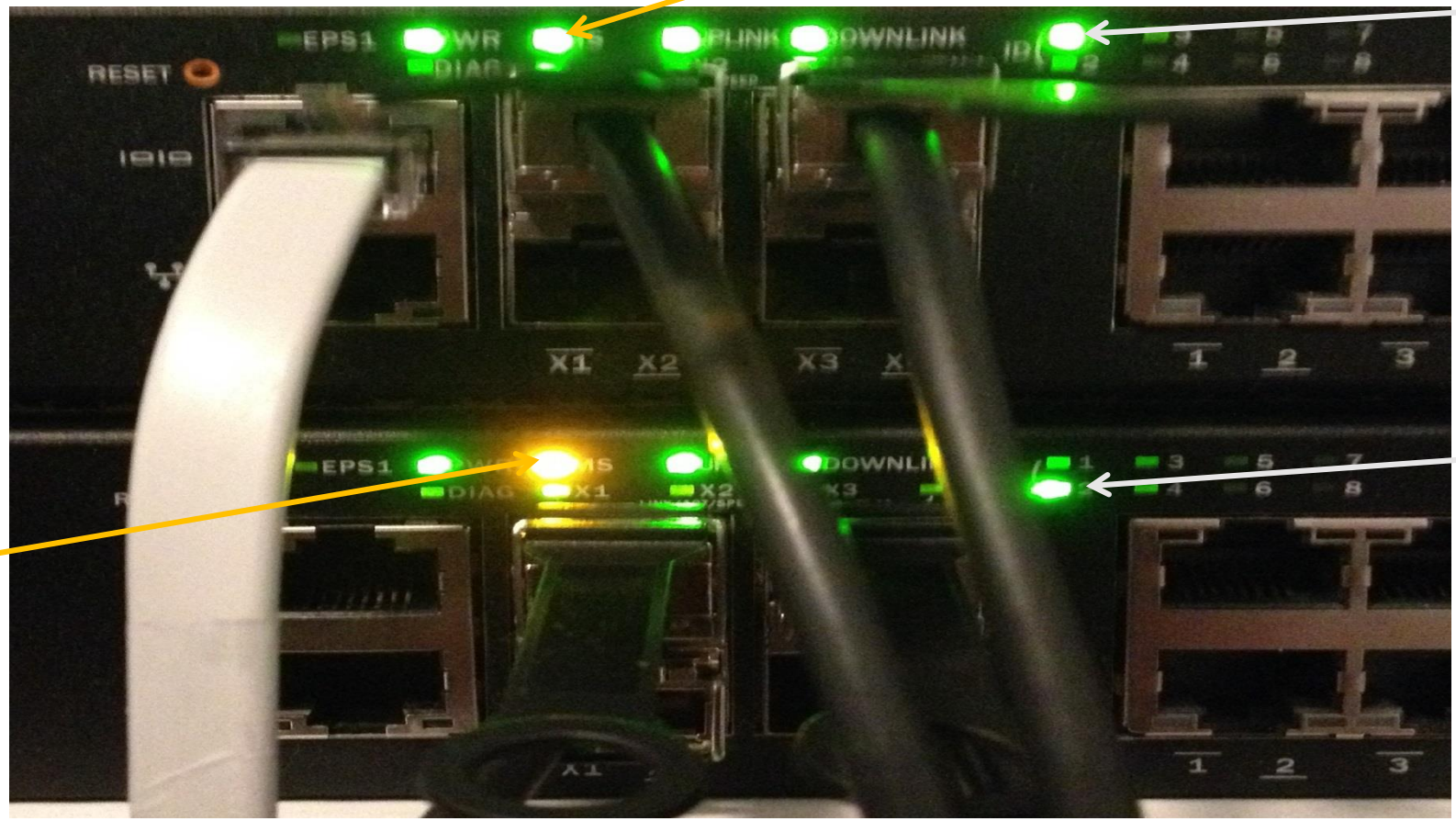
Stacking

Master UNIT
“Green”

UNIT ID 1

UNIT ID 2

Standby UNIT
“Amber”



Ruckus™

Security

- Username and password
  - username admin password St0p@tTh3Do0r
- Enable Superuser
  - enable super-user-password L3tme!nNow
- Authentication, Authorization, and Accounting (aaa)
  - aaa authentication web-server default local
  - aaa authentication enable default enable
  - aaa authentication login default local
  - aaa authentication login privilege-mode
  - enable aaa console

Time

- Clock set
  - clock set 08:45:25 09-02-2016
  - Done at the # prompt
- Setting DST and timezone
  - clock summer-time
  - clock timezone us Central
- Setting NTP Servers
  - ntp
    - » server 129.6.15.28
    - » server 129.6.15.29
    - » server 129.6.15.30

Neighbor Protocols

- Foundry Discovery Protocol (FDP)
  - Discovers Brocade FastIron and NetIron Products
  - fdp run
- Cisco Discovery Protocol (CDP)
  - Discovers Cisco devices
  - cdp run
  - cdp output is viewed in fdp output
- Link Layer Discovery Protocol (LLDP)
  - Discovers any device running the standard protocol. Most support it, but not always on by default
  - lldp run

Neighbor Protocols - Verification

- show fdp neighbor

```
SSH@Lab-6610#show fdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
(*) indicates a CDP device

   Device ID         Local Interface Holdtm Capblty Platform    PortID
   --------------    --------------- ------ ------- ---------   ------
(*)Lab-ESXi6-A       ethernet1/1/21   146    S       VMware ESX  vmnic1
(*)Lab-ESXi6-A       ethernet1/1/35   146    S       VMware ESX  vmnic0
(*)LAB-ESXi6-B       ethernet1/1/36   139    S       VMware ESX  vmnic0
(*)Cisco_SW.lab.loca ethernet1/1/43   177    S I     cisco WS-C3 FastEthernet1/0/23
(*)Cisco_SW.lab.loca ethernet1/1/44   177    S I     cisco WS-C3 FastEthernet1/0/24
   Edge-Switch       ethernet1/1/48   131    Router  ICX6450-C12 ethernet1/2/2
   Lab-6450          ethernet1/3/1    137    Switch  ICX6450-48  ethernet1/2/1
   Lab-7450          ethernet1/3/2    169    Router  ICX7450-24  ethernet1/2/3
```

Ruckus™

Neighbor Protocols - Verification

- show lldp neighbor

```
SSH@Lab-6610#show lldp neighbor
Lcl Port Chassis ID      Port ID          Port Description          System Name
1/1/43   001b.906b.af80 Fa1/0/23         FastEthernet1/0/23        Cisco_SW.lab.~
1/1/44   001b.906b.af80 Fa1/0/24         FastEthernet1/0/24        Cisco_SW.lab.~
1/1/45   0019.bb9e.2dc0 23               23                        ProCurve_2810
1/1/46   000f.065b.2c00 000f.065b.2c17   Port 23                   Nortel_5510
1/1/48   cc4e.2409.c1e6 cc4e.2409.c1f4   GigabitEthernet1/2/2      Edge-Switch
1/3/1    748e.f8ed.5900 748e.f8ed.5931   10GigabitEthernet1/2/1    Lab-6450
1/3/2    cc4e.2488.7cc8 cc4e.2488.7ce3   10GigabitEthernet1/2/3    Lab-7450
```

Ruckus™

Neighbor Protocols - Verification

- show lldp neighbor detail

```
SSH@Lab-6610#show lldp neighbor detail
Local port: 1/1/43
  Neighbor: 001b.906b.af99, TTL 115 seconds
    + Chassis ID (MAC address): 001b.906b.af80
    + Port ID (interface name): "Fa1/0/23"
    + Time to live: 120 seconds
    + System name          : "Cisco_SW.lab.local"
    + System description   : "Cisco IOS Software, C3750 Software (C3750-IPSERVI\
                             CESK9-M), Version 12.2(55)SE10, RELEASE SOFTWARE \
                             (fc2) Technical Support: http://www.cisco.com/tec\
                             hsupport Copyright (c) 1986-2015 by Cisco Systems\
                             , Inc. Compiled Wed 11-Feb-15 11:40 by prod_rel_t\
                             eam"
    + Port description     : "FastEthernet1/0/23"
    + System capabilities : bridge, router
      Enabled capabilities: bridge
    + Management address (IPv4): 10.10.10.253
    + 802.3 MAC/PHY        : auto-negotiation enabled
      Advertised capabilities: 10BaseT-HD, 10BaseT-FD, 100BaseTX-HD,
                               100BaseTX-FD
      Operational MAU type   : 100BaseTX-FD

Local port: 1/1/44
  Neighbor: 001b.906b.af9a, TTL 116 seconds
    + Chassis ID (MAC address): 001b.906b.af80
    + Port ID (interface name): "Fa1/0/24"
    + Time to live: 120 seconds
    + System name          : "Cisco_SW.lab.local"
    + System description   : "Cisco IOS Software, C3750 Software (C3750-IPSERVI\
                             CESK9-M), Version 12.2(55)SE10, RELEASE SOFTWARE \
```

MAC Address

Code Version

IP Address

Ruckus™

Simple Network Management Protocol (SNMP)

- SNMP Versions
  - Version 1 – very unsecure and outdated
  - Version 2c – replaces Version 1, but still unsecure
  - Version 3 – Newest version. Most secure
- Required for BNA integration (version 2c or 3)

SNMP Version 3 Configuration

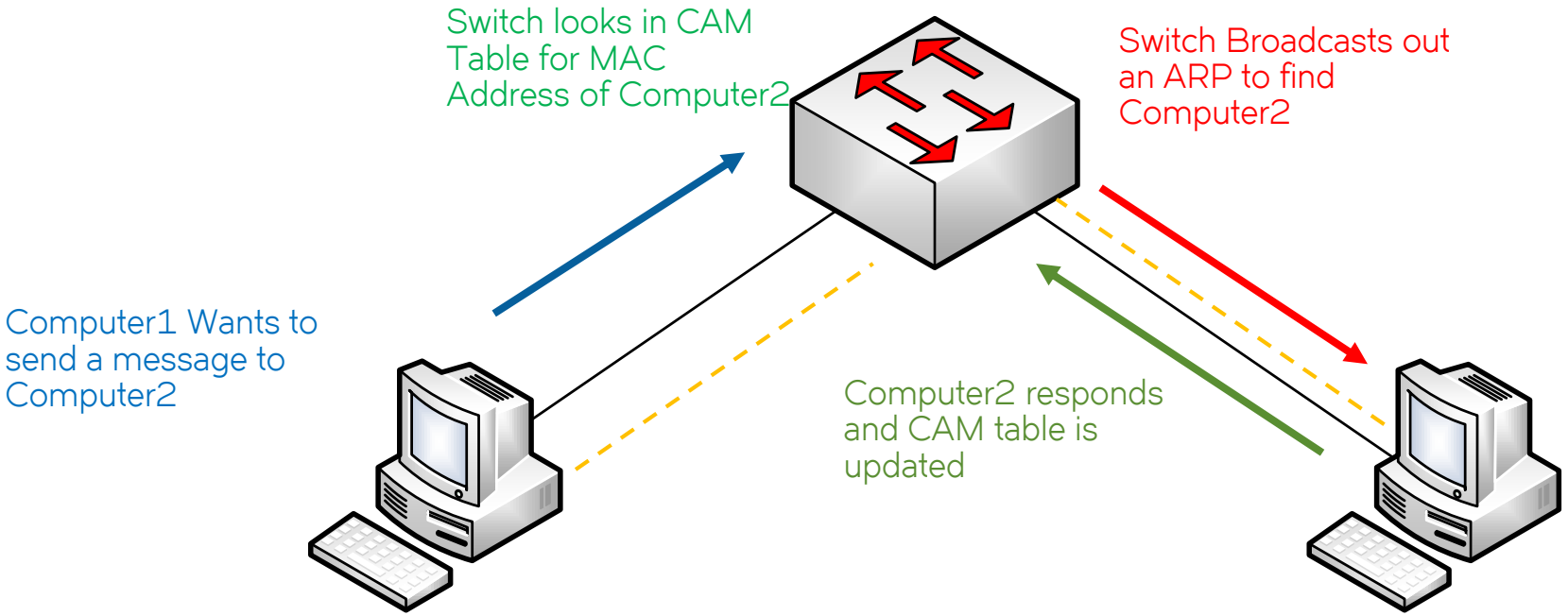
- Create the group and give privileges
  - snmp-server group admin v3 auth read all write all
- Create the username, password, and encryption
  - snmp-server user bna-snmp admin v3 auth sha SNMPpass1!# priv aes SNMPcrypt0@#12
- Allow the server access with the above access
  - snmp-server host 10.0.0.5 version v3 priv bna-snmp

Ruckus™

VLANs

- VLANs are required for Layer 2 traffic to pass
- VLAN 1 is the default VLAN
- VLANs create broadcast domains to segregate network traffic
- Each VLAN should have a unique subnet assigned
- VLAN numbers can be from 1 to 4091 (4092 – 4095 are reserved)

VLANs



MAC Address: aaaa.bbbb.cccc
IP Address: 10.0.0.5
Subnet Mask: 255.255.255.0
Gateway: 10.0.0.1

MAC Address: dddd.eeee.1111
IP Address: 10.0.0.6
Subnet Mask: 255.255.255.0
Gateway: 10.0.0.1

VLANs

- Creating a VLAN
  - config t
  - vlan 10 name Data

- Once the VLAN is created, ports can be added, spanning-tree can be configured, and a virtual Ethernet (VE) interface can be created.

VLANs - Adding Ports

- Tagged ports
  - Ports that will have an 802.1q tag in the header to identify the VLAN
  - Used to allow multiple VLANs to transverse one port
  - Mainly used for uplinks. Can be used for some AP and phone configurations

- Untagged ports
  - Ports that reference a VLAN tag and just pass the packets forward
  - Mainly used for end devices such as computers, printers, and cameras

VLANs – Adding Ports

- Tagged Ports

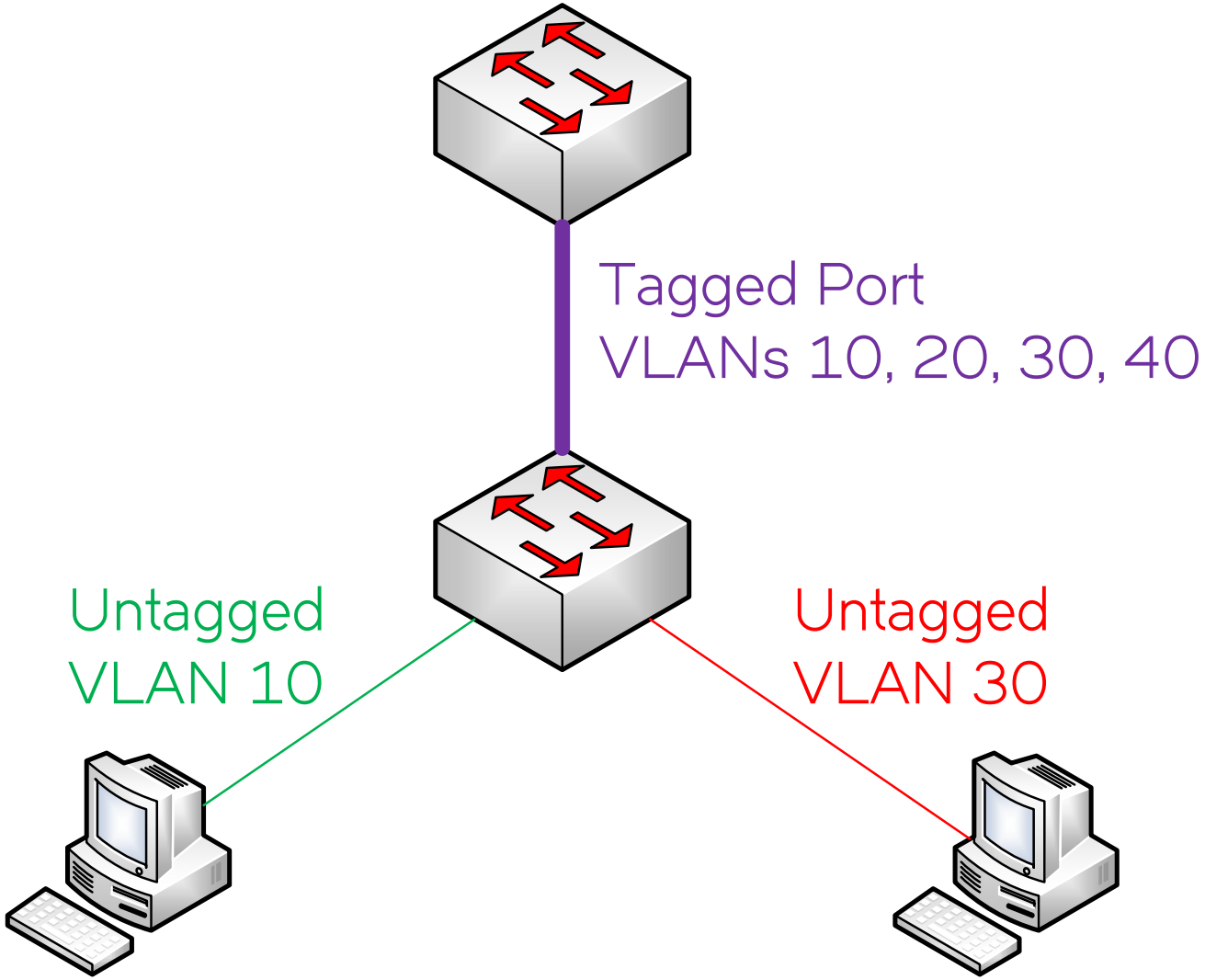
```
config t
vlan 10 name Data
tagged e 1/2/1
```

- Untagged Ports

```
config t
vlan 10 name Data
untagged e 1/1/1 to 1/1/24
```

Ruckus™

VLANs – Adding Ports



Ruckus™

VLANs – Spanning-tree

- Spanning-tree (802.1d)
  - Default spanning-tree on switches. Spanning-tree is not enabled du default on routing code
  - Supported on all switches
  - Convergence time is ~50 seconds

- Rapid Spanning-tree (802.1w)
  - Supported by most vendors, but not all are compatible
  - Convergence time is ~5 seconds

VLANs – Spanning-tree

- Spanning-tree can be per-VLAN or Single instance
  - Per-VLAN is recommended

- Set the priority on the switch you want to be the root.
  - Usually the Core or routing edge
  - Default priority is 32768
  - Lowers priority wins the election

VLANs – Spanning-tree

- Configuring PVST 802.1d

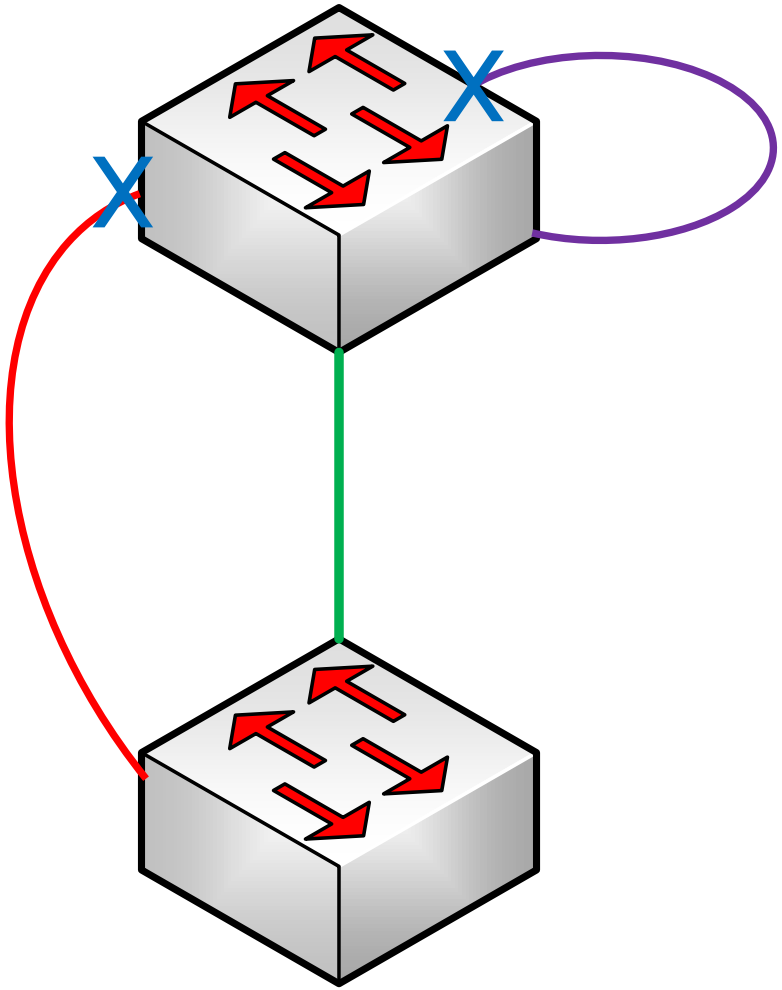
```
config t
vlan 10 name Data
spanning-tree
```

- Configuring PVST 802.1w

```
config t
vlan 10 name Data
spanning-tree 802.1w
```

Ruckus™

VLANs – Spanning-tree



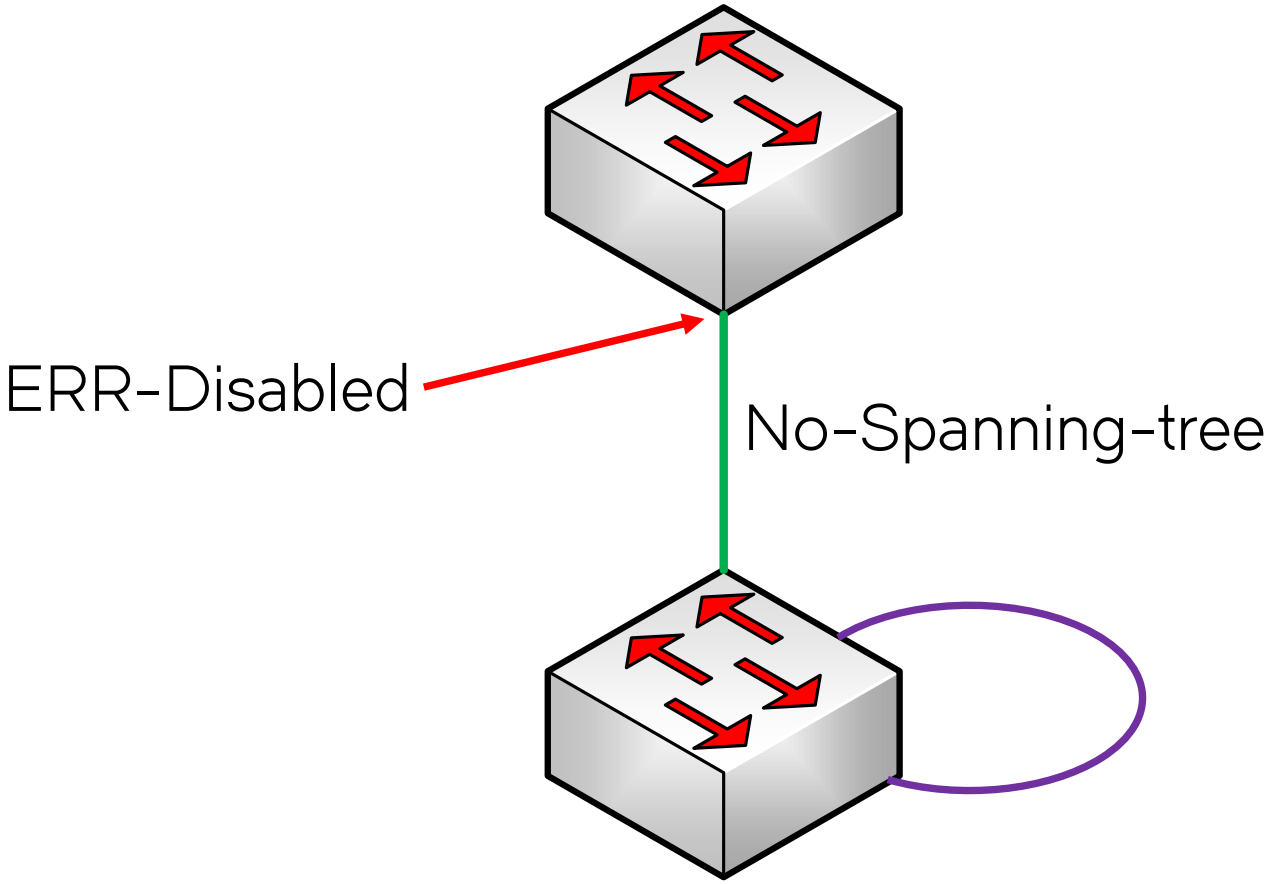
Loop-Detection

- There are two types of loop detection;
  - In Strict Mode, a port is disabled only if a packet is looped back to that same port. Strict Mode overcomes specific hardware issues where packets are echoed back to the input port. In Strict Mode, loop detection must be configured on the physical port.
  - In Loose Mode, loop detection is configured on the VLAN of the receiving port. Loose Mode disables the receiving port if packets originate from any port or VLAN on the same device. The VLAN of the receiving port must be configured for loop detection in order to disable the port.
- Use the loop-detection command to enable loop detection on a physical port (Strict mode) or a VLAN (Loose-mode)

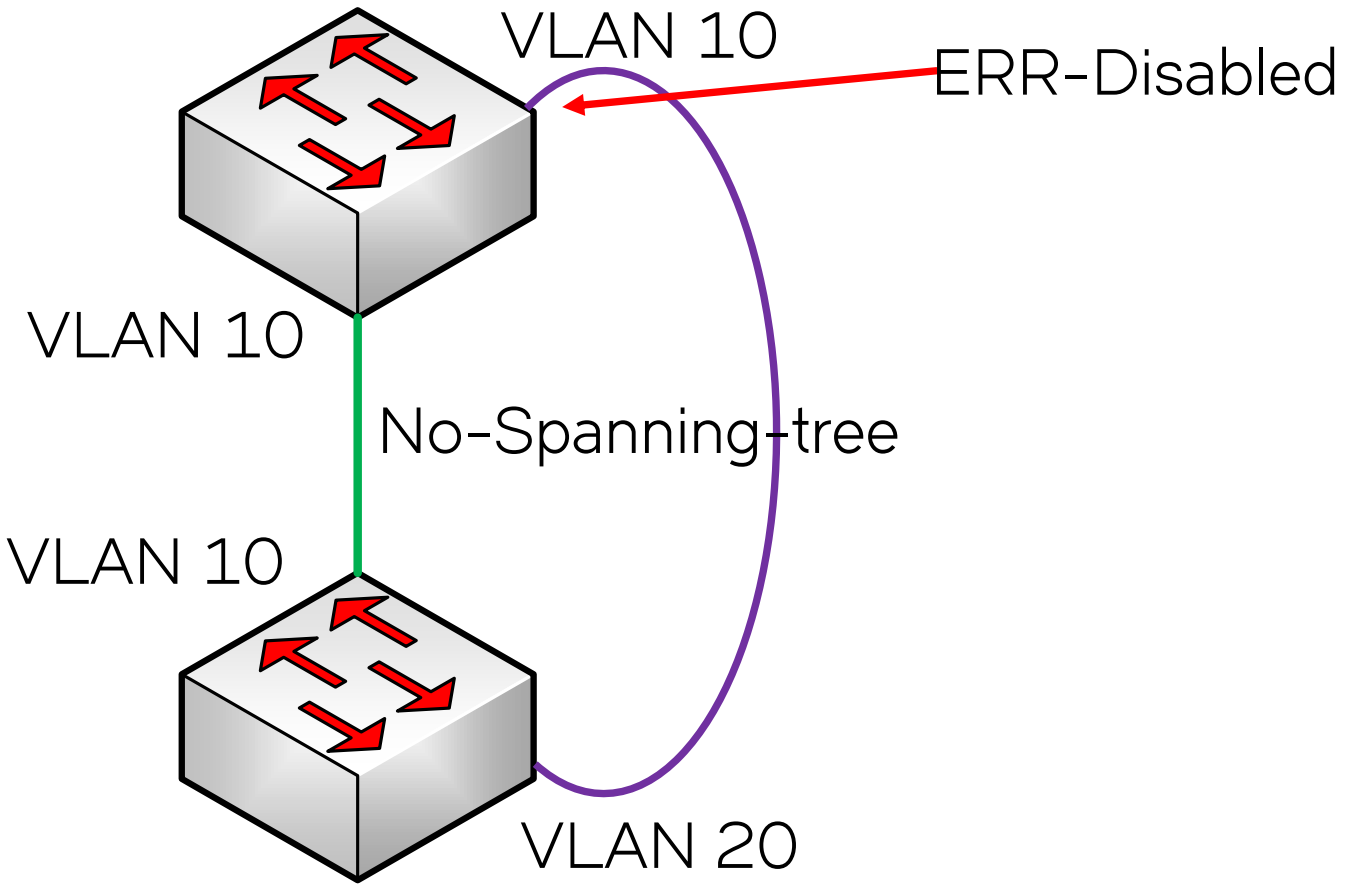
Loop-Detection

- Strict Mode
  - interface e 1/1/1
  - loop-detection
- Loose Mode
  - vlan 20
  - loop-detection

Loop-Detection – Strict Mode



Loop-Detection – Loose Mode



Ruckus™

VLANs – Router VE

- Router Virtual Ethernet (VE) Interfaces are a bridge between Layer 2 traffic and Layer 3 traffic.
- Usually used to define the default-gateway for a VLAN
- Create the router VE under the VLAN, then go to the VE and configure the IP Address.
- *A port must be defined under the VLAN before the router VE will be cone active for configuration.*

VLANs – Router VE

- Configuring the router VE
  - config t
  - vlan 10 name Data
  - tagged e 1/2/1
  - router-interface ve 10
  - exit
  - interface ve 10
  - ip address 10.10.10.1 255.255.255.0

VLAN – Sample Configuration

```
vlan 10 name Network by port
 tagged ethe 1/1/1 ethe 1/1/3 to 1/1/10 ethe 1/1/32 to 1/1/36 ethe 1/1/43 to 1/1/47 ethe 1/3/1 ethe 1/3/3
 untagged ethe 1/1/12 to 1/1/20
 router-interface ve 10
 spanning-tree 802-1w
 spanning-tree 802-1w priority 8192
!
vlan 20 name Voice by port
 tagged ethe 1/1/1 to 1/1/10 ethe 1/1/32 to 1/1/36 ethe 1/1/43 to 1/1/47 ethe 1/3/1 ethe 1/3/3
 router-interface ve 20
 spanning-tree 802-1w
 spanning-tree 802-1w priority 8192
!
vlan 30 name Guest by port
 tagged ethe 1/1/32 to 1/1/36 ethe 1/1/43 to 1/1/47 ethe 1/3/1 ethe 1/3/3
 router-interface ve 30
 spanning-tree 802-1w
 spanning-tree 802-1w priority 8192
```

Ruckus™

Layer 2 Switch Addressing

- Configuring IP Address
  - config t
  - ip address 10.0.1.14 255.255.255.0
- Configuring the Default Gateway
  - config t
  - ip default-gateway 10.0.1.1

Layer 3 Switch Static Routing

- Configuring the Default route
  - config t
  - ip route 0.0.0.0/0 10.0.14.1

- Configuring a static route
  - config t
  - ip route 2.2.2.2/32 10.10.10.253

Next Hop IP

Destination Network

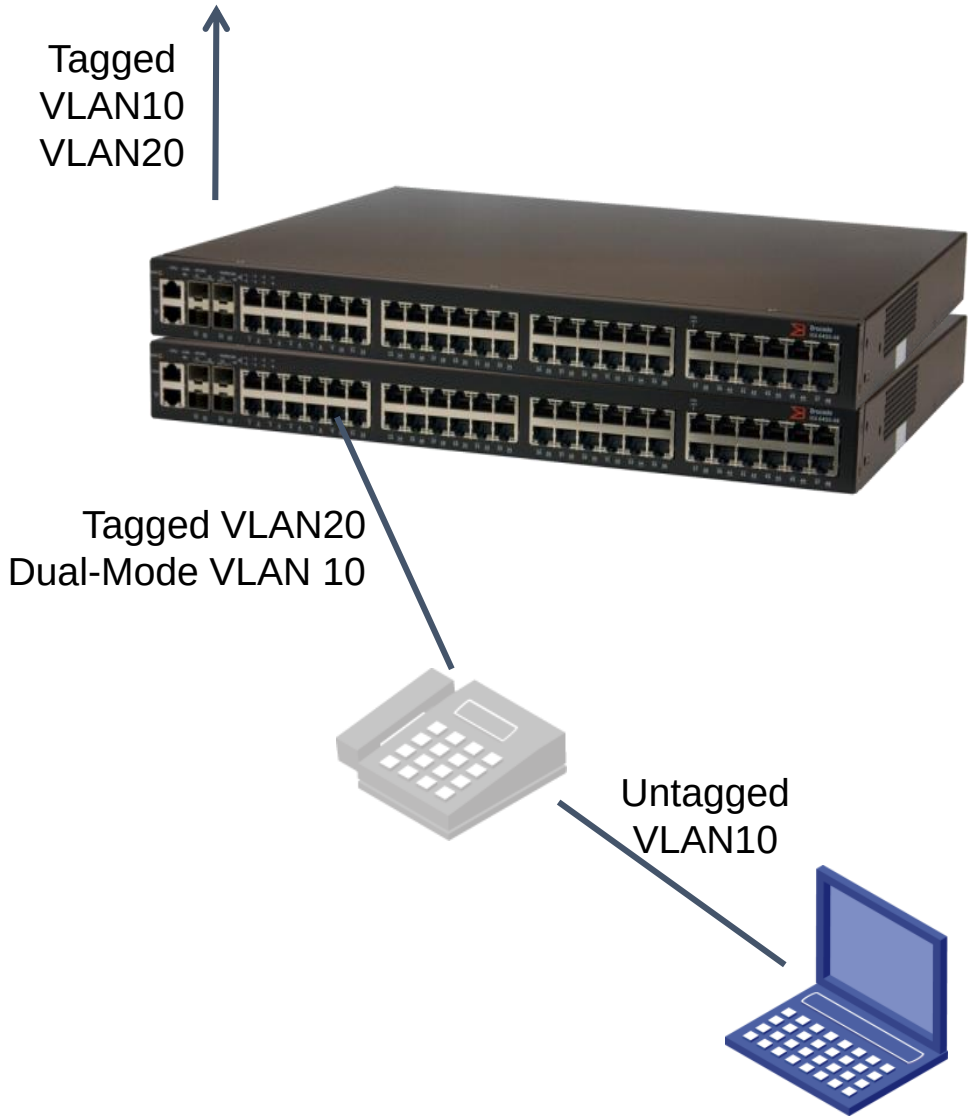
Dual-Mode Port

- A dual-mode port will accept a packet that is tagged or untagged
- Mainly used on ports with IP Phones, access points, or uplinks that need to account for a native VLAN.
- Configuration
  - Tag the port in all the VLANs you want to cross the link
  - Apply the dual-mode command to the VLAN that will pass untagged traffic.

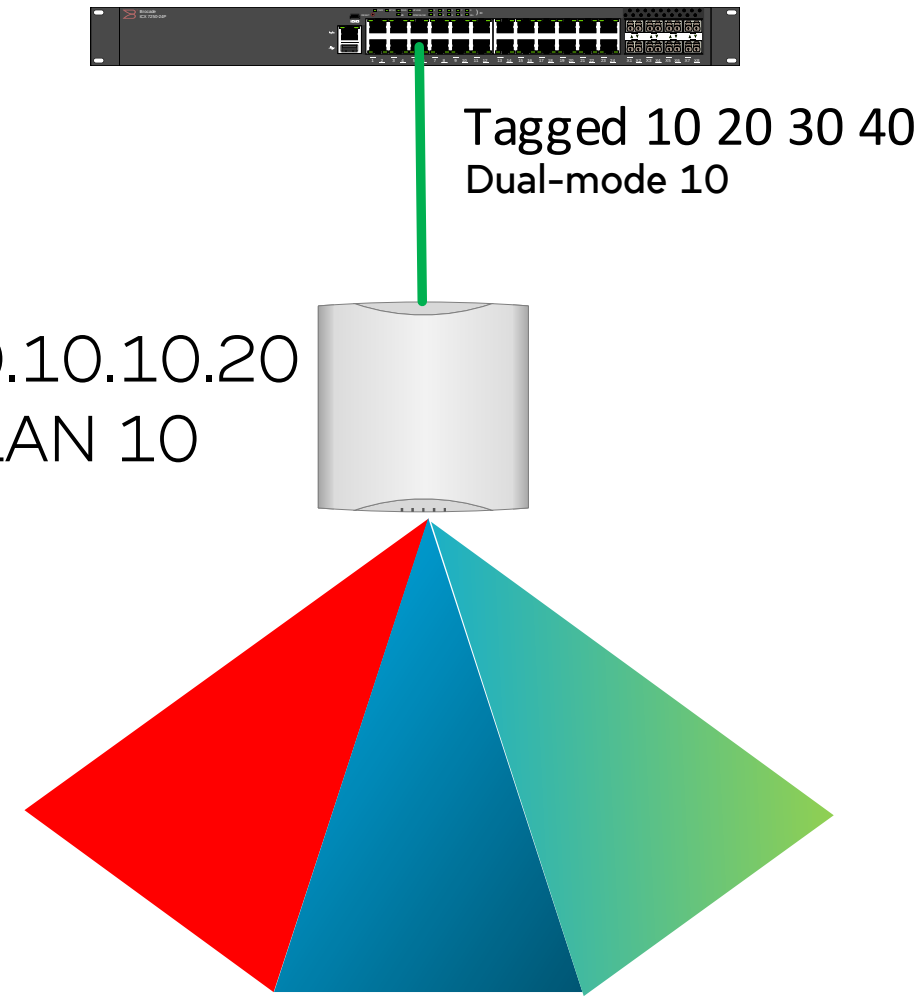
Dual-Mode Port

- config t
- vlan 10 20
- tagged e 1/1/1
- exit
- interface ethernet 1/1/1
- dual-mode 10

- VLAN 10 will be untagged



Dual-Mode Port



VLAN 10 – AP MGMT
VLAN 20 – Staff
VLAN 30 – Student
VLAN 40 - Guest

Ruckus™

Edge Port Configuration

- interface ethernet 1/1/1 to 1/1/24
- port-name Edge_Port
- loop-detection
- spanning-tree 802-1w admin-edge-port
- trust dscp

Ruckus™

Uplink Port Configuration

- interface ethernet 1/2/1
- port-name Uplink_Port
- spanning-tree 802-1w admin-pt2pt-mac
- trust dscp

Link Aggregation Configuration (LAG)

- Two types of LAG
  - Static
    - » Link comes up with no negotiation with peer
    - » Not secure or recommended, but necessary with some devices
  - Dynamic
    - » Link comes up with after LACP negotiation with peer
    - » Peer device must support Link Aggregation Control Protocol (LACP)

Link Aggregation Configuration (LAG)

- Static
  - config t
  - lag blue static id 1
  - ports ethernet 1/1 to 1/2
  - primary-port 1/1
  - deploy
- Dynamic
  - lag red dynamic id 1
  - ports ethernet 1/1 to 1/2
  - primary-port 1/1
  - deploy

Power Over Ethernet (PoE)

- PoE Configuration
  - config t
  - interface Ethernet 1/1/1
  - Inline power
- PoE Budget
  - LLDP
  - CDP (Cisco Phones)

PoE Software Upgrade

```
ICX6450-24P Switch#show inline power detail

Firmware
Version
--------
02.1.0
```

Check Firmware Version for each Unit

```
ICX6450-24P Switch#inline power install-firmware stack-unit 1 tftp 192.168.13.30
icx64xx_poeplus_02.1.0.fw
ICX6450-24P Switch#Flash Memory Write (8192 bytes per dot)
Automatic copy to member units:  2
....................
 tftp download successful stackId = 1 file name = poe-fw
```

Perform for each unit in stack

Quality of Service

- Class of Service (CoS)
  - Layer 2 marking of packets
  - 802.1p
  - Values 0 – 7
- DiffServ Code Point (DSCP)
  - Layer 3 marking of packets
  - Values 0 – 63
- Configuration
  - config t
  - interface Ethernet 1/2/1
  - trust dscp

DSCP to CoS Mappings

TABLE 18 Default DSCP to internal forwarding priority mappings

Internal forwarding priority		DSCP value
0 (lowest priority queue)	Best Effort	0 - 7
1		8 - 15
2		16 - 23
3		24 - 31
4		32 - 39
5	Voice	40 - 47
6		48 - 55
7 (highest priority queue)	Management	56 - 63

Ruckus™

Best Practices

VLANs

- VLAN 1 is the default VLAN
- Brocade uses the default VLAN as a “parking lot” for unused ports. It is different from the native VLAN in Cisco configurations.
- *Best Practice:* Change the default VLAN to an unused VLAN number.
- Example:
  - config t
  - default-vlan-id 1499

Security

- Telnet is enabled by default
- SSH is disabled by default
- *Best Practice:* Enable SSH and disable Telnet
- Example:
  - config t
  - crypto key generate rsa mod 1024
  - no telnet server

Preventing DoS Attacks

– Brocade device includes several defenses to combat the two most popular types of DoS attacks:

- **Smurf attacks** where ICMP is used and TCP SYN attacks which use a partial TCP 3-way handshake[1]
  - » Avoiding being an intermediary in a smurf attack

```
Brocade(config)# no ip directed-broadcast
```

  - » Avoiding being a victim in a smurf attack[2]

```
Brocade(config)# ip icmp burst-normal 5000 burst-max 10000 lockup 300
```

Syntax: `ip icmp burst-normal value burst-max value lockup seconds`

- **TCP SYN attacks** disrupt normal traffic flow by exploiting the way TCP connections are established
  - » To protect against participating in TCP SYN attacks[3]
    - – `Brocade(config)# ip tcp burst-normal 10 burst-max 100 lockup 300`

Ruckus™

IGMP Snooping

- IGMP Snooping is disabled by default
- *Best Practice:* Enable IGMP Snooping
- Example for Access Switches:
  - config t
  - ip multicast passive
- Example for Core Switch:
  - config t
  - ip multicast active

DHCP Snooping

– **DHCP snooping** enables the device to filter untrusted DHCP packets in a subnet which can:
  - Protect from Man-in-the-Middle attacks
  - Prevent malicious user posing as a DHCP server sending false DHCP server reply packets
  - Can stop unauthorized DHCP servers connected to the network (personal home routers)

```
config t
ip dhcp snooping vlan 2
ip dhcp snooping vlan 100
interface ethernet 1/1
 dhcp snooping trust
```

Ruckus™

QoS

- QoS is end-to-end
- At any point where there is a disconnect in QoS configuration, traffic could end up in the Best Effort queue.
- QoS settings only take effect when a link is saturated.

- CoS is on by default
- Apply DSCP to all interfaces
  - trust dscp

SFlow

- Sflow is a packet sampling technology used to monitor the network.
- Sflow is disabled by default
- Must be enabled globally and on the ports to monitor
- *Best Practice:* Enable on uplink ports
- Example (global configuration):
  - config t
  - sflow sample 8192
  - sflow destination 10.0.1.30
  - sflow enable

SFlow

- Example (port configuration):
  - config t
  - interface ethernet 1/3/1
  - sflow forwarding

- *Can be enabled on all ports. This is not recommended as it can be processor intensive. Use only when necessary for short periods.*

Questions?

Reference Material

Reference Material

- Documentation
  - support.ruckuswireless.com (login required)
  - my.brocade.com
- Training
  - training.ruckuswireless.com
  - my.brocade.com
- Exit Certified
  - Instructor led training
- NetAdmin Website
  - www.netadmin.us
  - NetAdmin YouTube Channel
  - NetAdmin Blog

Thank You