

Network Install Checklist

Technician:

Job #:

Client:

Date:

Cables

- Terminate all cables using the same standard (TIA-568B is best)
- Test each cable for faults
- No Ethernet cable runs longer than 100m
- Use shielded cables in areas with high EMI

Router

- Fill out your company's network planning sheet
- Connect WAN port to modem or internet port
 - If present, set the ISP-provided modem/router to bridge mode
 - If no bridge mode, set DMZv4 for the router's WAN address
- Router power is protected and conditioned
- Change router username and password
- Name router and note its location
- Check default gateway
 - If assigned a static WAN IP, configure router's WAN interface
 - IP address
 - Subnet mask
 - Gateway
 - DNS
 - VLAN tag (if needed)
- Set DNS server
- Set subnet mask to:
 - 255.255.255.0 for networks with less than 254 hosts
 - 255.255.254.0 for up to 510 hosts
- Back up configuration

IP Address Scheme

- Use DHCP
 - Use static only when required
- Set DHCP reservations for key equipment

VLAN

Use a VLAN only if needed; examples include:

- large surveillance systems
- running multiple high-definition media streams
- MoIP
- segregation for security
- isolating unsecure Internet of Things devices

- Default VLAN
 - Name left at "default"
 - Enable Inter-VLAN Routing unless isolation is desired
 - Set traffic to untagged for all ports
- Additional VLANs
 - Name the VLAN
 - Enable Inter-VLAN Routing if unicast must pass between VLANs
 - Set traffic to tagged for all ports
 - Set subnet mask
 - Set IP range
 - Set DNS

Core Switch

- Switch power is protected and conditioned
- Change switch username and password
- Name switch and note its location
- Connect to router (through uplink port if specified)
- Back up configuration

Spanning Tree Protocol

Use only if required (by Sonos, DirecTV, Tivo, Kaleidescape, and others)

- Araknis
 - Disable STP if not required
 - Set bridge priority to 4096
 - Set CST to off (by port, where needed)
 - Disable Auto Edge on every port involved with STP
- Pakedge
 - Enable Spanning Tree Admin Mode if STP is required
 - Set version to IEEE802.1w
 - Set bridge priority to 4096
 - Enable CST for port 1
 - Disable Auto Edge on every port involved with STP

Multicast

Only enable multicast if

- Certain network systems require it (MoIP, NVX, Wyrestorm, e.g.)
- IGMP will not break other network systems

- Araknis:
 - Enable IGMP snooping
 - Enable V2
 - Enable report suppression
 - Enable flood
 - Enable IGMP Snooping Status
 - Enable fast leave
 - Enable querier state
 - Set unregistered multicast to drop
- Pakedge:
 - Enable IGMP snooping Admin mode
 - Enable Fast Leave Admin Mode
 - Enable Report Suppression Mode
 - Enable IGMP Snooping Querier Admin Mode
 - Enable IGMP V2
 - Set Querier VLAN IP Address to 0.0.0.0
 - Enable Unregistered Multicast Drop

PoE

- Total power draw not higher than 85% of the power budget

VLANs

Use only if VLANs have been enabled in the router.

- Default VLAN
 - Enable Inter-VLAN routing if unicast must pass between VLANs
 - Set all port traffic to untagged
- Specialized VLAN
 - Name the VLAN for its purpose
 - Specify IP address and range
 - Set DNS
 - Specify trunk port
 - Connect trunk port to the router
 - Set trunk port traffic to Tagged
 - Specify Access port(s)
 - Connect access ports to other gear
 - Set access port traffic to Untagged
- Araknis
 - Set DNS Server mode to static
- Pakedge
 - Enable multicast routing if multicast must pass between VLANs

VPN

Use if remote access is needed beyond what OvrC provides. Avoid using Port Forwarding.

- Establish VPN standard
 - Enable OpenVPN
 - Create DDNS to use with OpenVPN
 - Ensure the OpenVPN port 1194 is open from outside the network
 - Download the OpenVPN config
 - If using Dynamic DNS, verify it resolves to the correct public IP address
 - Verify with NSlookup or ping the DDNS address
 - Disable PPTP VPN for security
- If using an ISP-provided router in addition to your Araknis/Pakedge:
 - Set ISP router above with DMZ, IP passthrough, or bridge mode

Branch Switches

- Switch power is protected and conditioned
- Change switch username and password
- Name switch and note its location
- Connect to core switch (through uplink port if specified)
- Back up configuration

Spanning Tree Protocol

- Match settings from core switch
- Araknis
 - Disable STP if not required
 - Set bridge priority to 8192
 - Set CST to off (by port, where needed)
 - Disable Auto Edge on every port involved with STP
- Pakedge
 - Enable Spanning Tree Admin Mode if STP is required
 - Set version to IEEE802.1w
 - Set bridge priority to 8192
 - Enable CST for port 1
 - Disable Auto Edge on every port involved with STP

PoE

- Total power draw not higher than 85% of the power budget

VLANs

Use only if VLANs have been enabled in the router.

- Default VLAN
 - Enable Inter-VLAN routing if unicast must pass between VLANs
 - Set all port traffic to untagged
- Specialized VLAN
 - Name the VLAN for its purpose
 - Specify IP address and range
 - Set DNS
 - Specify trunk port
 - Connect trunk port to the router
 - Set trunk port traffic to Tagged
 - Specify Access port(s)
 - Connect access ports to other gear
 - Set access port traffic to Untagged
 - Araknis
 - Set DNS Server mode to static
 - Pakedge
 - Enable multicast routing if data passes between VLANs

Each Access Point

- Change AP username and password
- Connect to core switch
- Set lease renewal based on expected use
- Disable band steering
- Enable fast roaming with multiple access points
 - Pakedge: Enable Fast BSS Transition (802.11r)
- AP power is protected and conditioned
- Back up configuration

Bands

- Set 2.4 GHz width to 20 MHz
- Set 5 GHz to
 - 40 MHz width (UNII-1 channels only)
 - 80 MHz (UNII-1 and -3 channels)
- For the home network, the 2.4GHz and 5 GHz bands have
 - The same non-default name
 - WPA2-PSK
 - The same password
 - The password is a long phrase
 - Broadcast SSID enabled
- For the guest network, the 2.4 GHz and 5 GHz bands have
 - The same name (clearly labeled for guests)
 - WPA2-PSK
 - The same password (not the same as the home network)
 - The password is a long phrase
 - Broadcast SSID enabled
 - Client isolation enabled unless otherwise requested
- Set transmission power so that transition areas have RSSI at
 - 70dB for 2.4 GHz
 - 65dB for 5 GHz

Channels

- Survey the site to determine cleanest channels
- Assign those channel statically (do not use auto)
- Assign all channels in a proper triangle pattern

Managed Power Unit

- Plug MPU into power source.
 - Alternatively, plug into a UPS that is plugged into the source.
- Plug MPU network cable into core switch.
- Name each outlet for the device it powers.
- Auto-reboot
 - Enabled
 - Pings customized per outlet
 - Settings customized per outlet
- Network devices power controls
 - Set with proper power-on delay
 - Set only to reboot, not power off
- Back up configuration

OvrC

- Customer and site data added
- Claim the Araknis/Pakedge router or OvrC Pro Hub first
 - Ensure it has claimed all other devices on the network
- Name each device clearly
- Install and customize OvrC Home

For additional information,
please visit our Tech Community
at tech.control4.com

